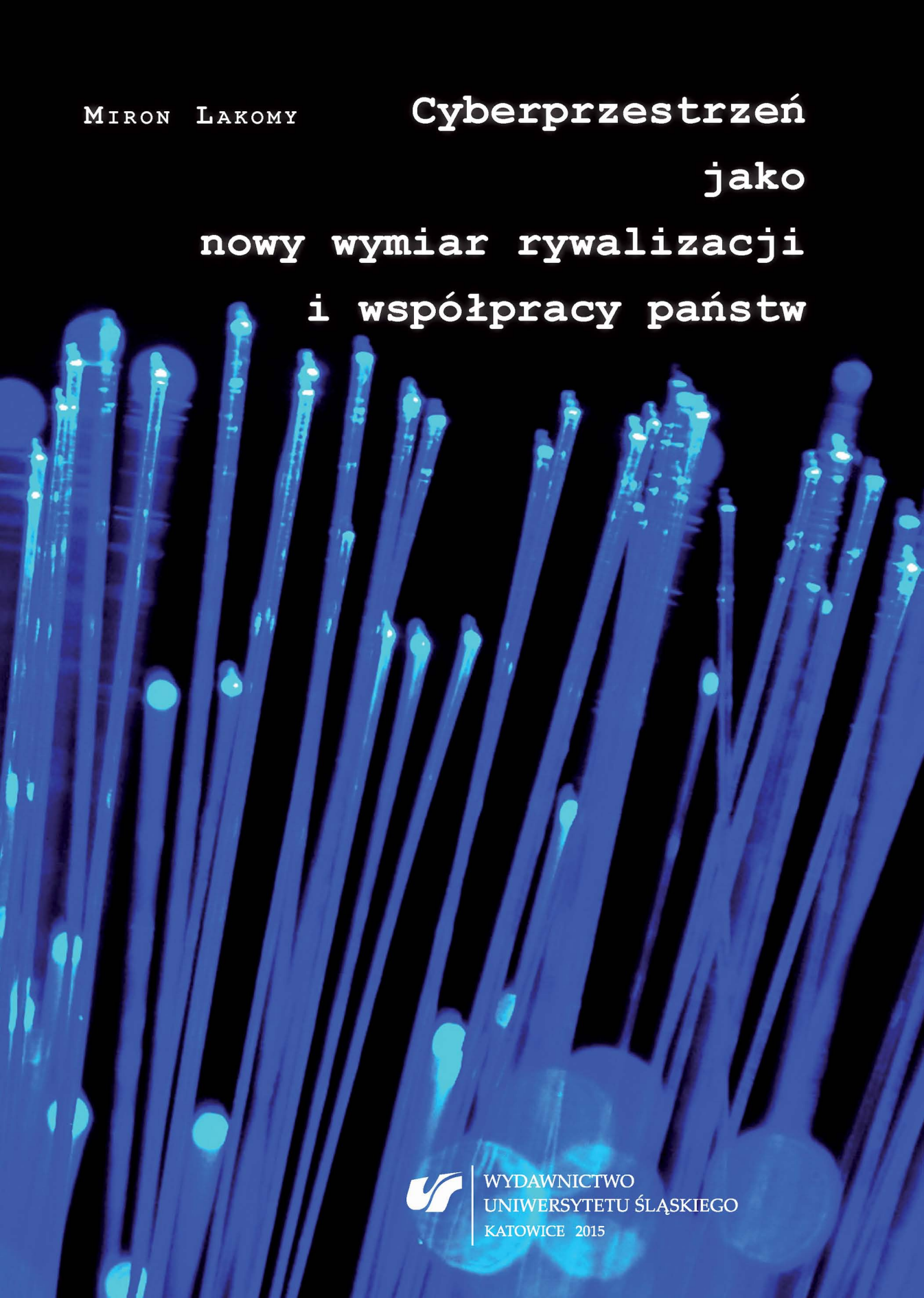
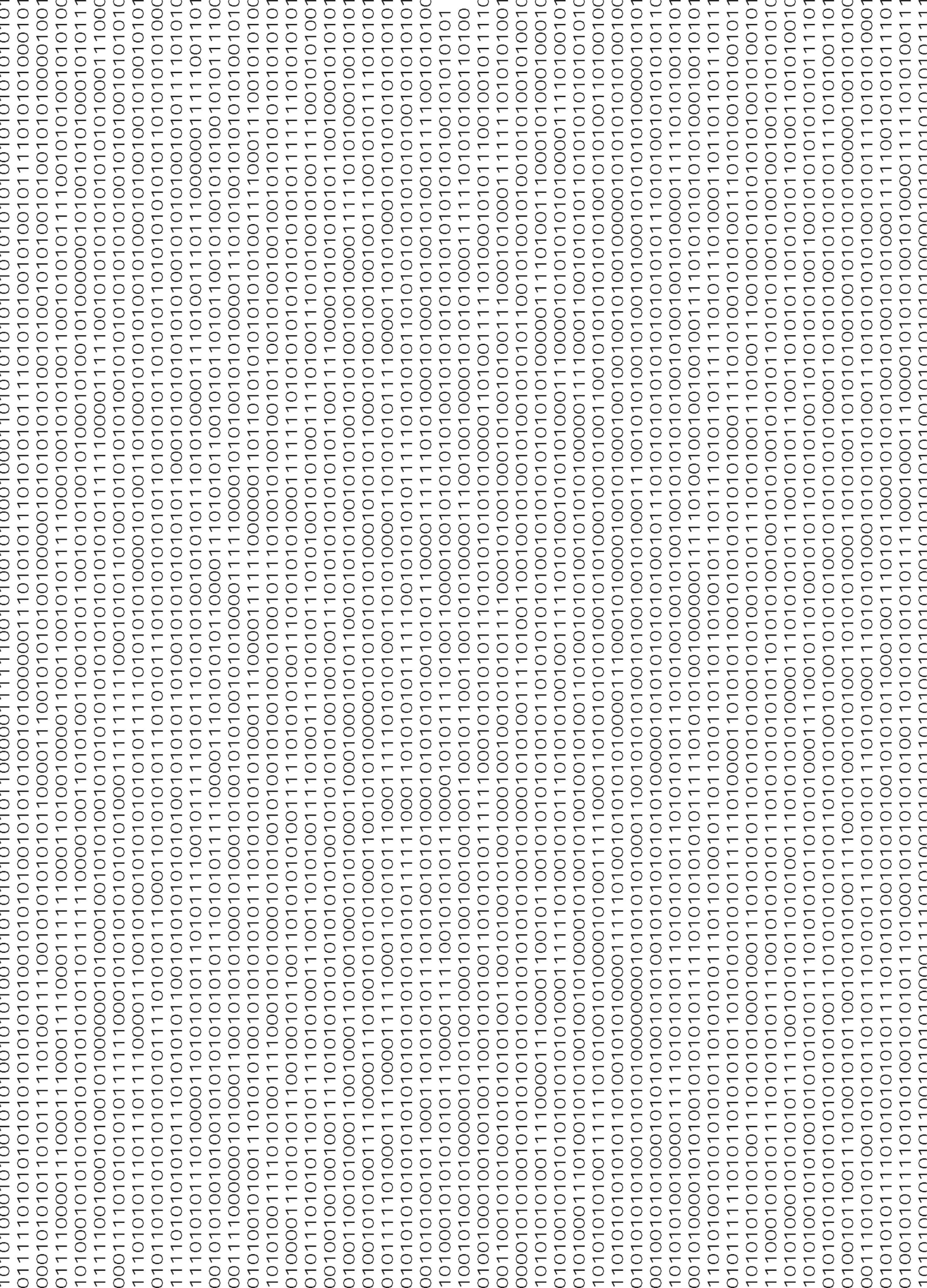
Miron Lakomy

Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw



WYDAWNICTWO
UNIWERSYTETU ŚLĄSKIEGO
KATOWICE 2015



Cyberprzestrzeń
jako nowy wymiar rywalizacji
i współpracy państw

PRACE
NAUKOWE

UNIWERSYTETU
ŚLĄSKIEGO
W KATOWICACH

NR 3293

Miron Lakomy

Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw

Wydawnictwo Uniwersytetu Śląskiego • Katowice 2015

Redaktor serii: Nauki Polityczne
Mariusz Kolczyński

Recenzent
Michał Chorośnicki

Fotografia na okładce: Mike Seyfang / „Fibre" | www.flickr.com

Redakcja: Katarzyna Wyrwas
Projekt okładki: Kamil Gorlicki
Redakcja techniczna: Barbara Arenhövel
Korekta: Lidia Szumigała
Łamanie: Marek Zagniński

ISSN 0208-6336
ISBN 978-83-8012-357-1
(wersja drukowana)
ISBN 978-83-8012-358-8
(wersja elektroniczna)

Wydawca
Wydawnictwo Uniwersytetu Śląskiego
ul. Bankowa 12B, 40-007 Katowice
www.wydawnictwo.us.edu.pl
e-mail: wydawus@us.edu.pl

Wydanie I. Ark. druk. 30,5. Ark. wyd. 43,5.
Papier offset. kl. III, 90 g. Cena 52 zł (+ VAT)

Druk i oprawa: „TOTEM.COM.PL Sp. z o.o." Sp.K.
ul. Jacewska 89, 88-100 Inowrocław

Spis treści

Wstęp

Bezprecedensowy rozwój naukowo-techniczny, który rozpoczął się po drugiej wojnie światowej, w ciągu kilku dekad doprowadził do rewolucyjnych zmian we wszystkich sferach życia człowieka. Począwszy od komunikacji, przez rozrywkę, życie społeczne i gospodarcze, aż po procesy polityczne, nowe technologie informacyjne i komunikacyjne, zgodnie z przewidywaniami części deterministów technologicznych (zob. Bimber, 1994), w niespotykany dotychczas sposób zmieniły oblicze świata. Pojawienie się komputerów oraz Internetu, a także innych urządzeń i usług korzystających z dorobku szeroko pojętej teleinformatyki doprowadziło na przełomie XX i XXI wieku do sytuacji, w której ludzkość stała się od nich *de facto* uzależniona. O skali tego zjawiska świadczył fakt, iż w ciągu ostatnich pięciu lat liczba użytkowników Internetu uległa podwojeniu i w 2013 roku wyniosła ok. 2,749 miliarda osób. Oznacza to, że niemal 40% ludzkości regularnie czerpało z potencjału globalnej sieci komputerowej (*Key indicators*, 2013). Jest ona powszechnie używana na masową skalę nie tylko przez pojedynczych użytkowników, ale także przez podmioty sektora prywatnego i publicznego. Z jej możliwości korzystają bowiem organizacje rządowe i pozarządowe, przedsiębiorstwa, korporacje transnarodowe, instytucje administracji publicznej, a nawet siły zbrojne. Nowe technologie na początku XXI wieku stały się więc instrumentem wykorzystywanym powszechnie we wszelkich możliwych wymiarach i płaszczyznach funkcjonowania państw i społeczeństw.

Niespotykany wcześniej w historii ludzkości postęp naukowo-techniczny nie wiąże się jednak wyłącznie z samymi korzyściami. Środowisko naukowe, przede wszystkim w państwach zachodnich, jeszcze w okresie głębokiej zimnej wojny zauważyło, iż rewolucja informatyczna będzie prowadzić do powstawania nowych wyzwań, zarówno w wymiarze politycznym, społecznym, gospodarczym, kulturowym, jak i *stricte* wojskowym. Równolegle temat ten stał się

niezwykle popularny w literaturze fantastyczno-naukowej, która w wielu wypadkach skupiła się na próbach przewidzenia negatywnych konsekwencji pojawienia się nowych technologii. W dyskusji naukowej, która rozgorzała na dobre niemal trzy dekady temu, upowszechniły się jednak głosy i postawy często skrajne, przeceniające wagę problemów w tym zakresie lub niedoceniające jej. Zdaniem części badaczy skala negatywnych następstw rewolucji informatycznej stała się tak duża, iż pojawiło się ryzyko wystąpienia swoistego „cyberarmageddonu", określanego także mianem „elektronicznego Pearl Harbor" lub „elektronicznego Waterloo" (zob. np. Guisnel, 2002: 53; Adams, 2001; Cordesman, Cordesman, 2001: 2; Krepinevich, 2012: 2; Eriksson, Giacomello, 2006: 226). Scenariusz ten zakłada możliwość dokonania strategicznego uderzenia w szeroko rozumianej cyberprzestrzeni, które doprowadziłoby do paraliżu krytycznej infrastruktury państw (zob. Lucky, 2010: 25; Heinl, 2012; Lewis, 2006), przesiąkniętej współcześnie urządzeniami opartymi na ICT (ang. *Information and Communication Technology*)[1]. W literaturze specjalistycznej częstokroć wskazuje się na rosnące zagrożenia dla funkcjonowania sieci elektroenergetycznych, sektora finansowego bądź systemu obronnego, co mogłoby skutkować m.in. odcięciem dostaw energii elektrycznej w skali całego kraju, kryzysem gospodarczym bądź utratą zdolności prowadzenia działań wojennych. Daniel T. Kuehl pisał w tym kontekście, iż Stany Zjednoczone mogą zostać pokonane nawet w ciągu „pierwszej nanosekundy" kolejnego konfliktu zbrojnego. Można tu także wspomnieć o artykule naukowym opublikowanym w 1997 roku, który autorzy zatytułowali wymownie: *Terroryzm informacyjny: Czy możesz zaufać swojemu tosterowi?* (Devost, Houghton, Pollard, 1997: 63—78). Tego typu katastroficzne wizje jak na razie się nie potwierdziły, co bywa podkreślane przez inną grupę ekspertów. Ci z kolei twierdzą, iż problemy na tym tle są często mocno przejaskrawione, a skala wyzwań dla bezpieczeństwa narodowego i międzynarodowego jest w rzeczywistości stosunkowo niewielka (zob. Weimann, 2005; Gartzke, 2013: 41—73).

Wraz z rozprzestrzenianiem się globalnej tkanki systemów teleinformatycznych pojawia się jednak coraz więcej praktycznych przykładów szkodliwego wykorzystania technologii ICT. Pierwsze incydenty tego typu miały miejsce jeszcze w czasie zimnej wojny, choć rozpowszechniły się na masową skalę dopiero na przełomie XX i XXI wieku, wraz z postępem procesów komputeryzacji i informatyzacji[2]. Początkowo były one związane z działalnością

[1] Termin ten wykorzystywany jest od niedawna, przyjął się jednak jako najpełniejsze ujęcie związku pomiędzy rozwiązaniami telekomunikacyjnymi a informatycznymi. W Polsce ICT utożsamia się z reguły z teleinformatyką.

[2] Komputeryzacja polega na zastępowaniu tradycyjnych metod funkcjonowania urzędów państwowych systemami komputerowymi, m.in. przez wprowadzanie elektronicznych baz danych, formularzy internetowych czy listów e-mail jako podstawowych metod komunikacji. Informatyzacja natomiast polega na wykorzystaniu systemów informatycznych do analizy i przetwarzania wprowadzonych danych. Zob. Lakomy, 2011a: 141.

raczej niegroźnego środowiska pasjonatów informatyki, z którego wywodzili się pierwsi hakerzy. Z czasem komputery oraz ich sieci zaczęły być jednak wykorzystywane przez cyberprzestępców, widzących w nich szansę na uzyskanie określonych korzyści osobistych. Równolegle technologie informacyjne i komunikacyjne zyskiwały coraz wyraźniejsze znaczenie polityczne, związane z wyodrębnieniem pierwszych grup haktywistów. Problemy z tym związane, mimo znacznej popularności w mediach (zob. Wall, 2007: 10—15) i kulturze masowej, przez wiele lat nie spotkały się ze zwiększonym zainteresowaniem społeczności międzynarodowej. Rządy poszczególnych państw, z wyjątkiem kilku pionierów w tej dziedzinie, nie dostrzegały szybko rosnącej skali wyzwań. Do przełomu w tym zakresie doszło dopiero w kwietniu i maju 2007 roku, kiedy Estonia jako pierwszy kraj na świecie została zaatakowana przez Internet w niespotykanym wcześniej stopniu. W wyniku trwającej trzy tygodnie kampanii cyberataków nie tylko zablokowano strony internetowe wielu instytucji publicznych, ale także naruszono wybrane elementy infrastruktury krytycznej (Miller, Kuehl, 2009). Jeszcze w tym samym roku we wrześniu Izrael udowodnił, iż cyberprzestrzeń zaczęła się stawać piątym teatrem wojny, obok lądu, morza, przestrzeni powietrznej i kosmicznej. W ramach operacji *Orchard* przeciwko Syrii dokonano sabotażu jej systemu obrony przeciwlotniczej, prawdopodobnie za pomocą włamania komputerowego. W kolejnych latach w sieci doszło do całej gamy innych bardzo poważnych incydentów, które potwierdzały skalę problemów wynikających z niewłaściwego zastosowania osiągnięć rewolucji informatycznej. Przykładowo w sierpniu 2008 roku towarzyszyły one konfliktowi zbrojnemu na Kaukazie. Na przełomie pierwszej i drugiej dekady XXI wieku potencjał nowych technologii został wykorzystany przeciwko Kirgistanowi oraz Iranowi. W tym ostatnim przypadku izraelskie i amerykańskie służby wywiadowcze zastosowały niezwykle zaawansowany, złośliwy program komputerowy *Stuxnet*, aby sabotować program atomowy reżimu ajatollahów. W podobnej sytuacji znalazły się również same Stany Zjednoczone, które stały się najpopularniejszym obiektem miliardów prób włamań komputerowych w ostatnich latach. Cyberataki posłużyły ponadto jako nowy sposób wywierania nacisku politycznego podczas napięć na Półwyspie Koreańskim, między innymi w latach 2011 i 2013.

Pojawia się więc pytanie, jak należy interpretować tego typu wydarzenia oraz jakie jest ich znaczenie dla rozmaitych obszarów życia człowieka i zbiorowości ludzkich. Badania w tym zakresie prowadzi się z wielu rozmaitych perspektyw badawczych. Nauki ścisłe i techniczne skupiają się m.in. na takich kwestiach, jak zabezpieczenia komputerowe, funkcjonalność infrastruktury teleinformatycznej czy nowe technologie telekomunikacyjne. Od lat sfera ta budzi także rosnące zainteresowanie przedstawicieli nauk społecznych, którzy dostrzegają coraz wyraźniejszy związek między postępem naukowo-technicznym a procesami politycznymi, gospodarczymi czy kulturowymi. Jednym z najważ-

niejszych punktów przecięcia badań z obu tych perspektyw jest znaczenie incydentów komputerowych dla bezpieczeństwa narodowego i międzynarodowego. W burzliwej dyskusji poświęconej tym zagadnieniom powstało wiele nowych, wcześniej nieznanych kategorii naukowych, takich jak *cyberterroryzm* lub *cyberwojna*. W zamyśle ich twórców mają one oddawać sens nowych zagrożeń, wynikających z proliferacji technologii teleinformatycznych. Próżno jednak szukać zgody środowiska ekspertów co do jednoznacznego rozumienia tych terminów, a szerzej: co do stosowanej siatki pojęciowej. Nawet w sprawach, które wydawałyby się z pozoru oczywiste, trudno o konsensus, niełatwo bowiem doszukać się podzielanych powszechnie konkluzji co do skali tych wyzwań czy ich bezpośrednich skutków np. dla współczesnej formy konfliktów zbrojnych. Należy się więc zgodzić ze słowami Myriam Dunn-Cavelty (2008: 14), która stwierdziła, iż terminologia ery informacyjnej jest „nieprecyzyjna, dwuznaczna i nieuchwytna".

Jedną z najbardziej kontrowersyjnych kwestii w tej debacie jest rosnąca rola cyberprzestrzeni w stosunkach międzynarodowych. Z pozoru jest to konstatacja naturalna, po bliższym przyjrzeniu okazuje się jednak, iż brak jest pogłębionych analiz, które przy wykorzystaniu narzędzi badawczych właściwych nauce o stosunkach międzynarodowych podjęłyby się sprawdzenia, w jaki sposób ich uczestnicy czerpią z potencjału sieci oraz z jakimi wiąże się to konsekwencjami. Badacze z reguły skupiają się tu na wycinkowych problemach, co utrudnia sformułowanie jednoznacznych wniosków na temat trendów i procesów o zasięgu globalnym. Zdecydowanie bogatsza dyskusja, jak wspomniano, dotyczy zagrożeń teleinformatycznych i ich znaczenia dla bezpieczeństwa narodowego i międzynarodowego, niewiele jest natomiast analiz, które wpisywałyby te zagadnienia w szersze ramy działań poszczególnych podmiotów funkcjonujących w środowisku międzynarodowym. Praca ta jest więc reakcją na tę konstatację. Dostrzegając kolejne incydenty komputerowe, które w coraz większym stopniu zagrażają bezpieczeństwu państw, warto zadać pytanie, czy cyberprzestrzeń nie staje się nową sferą ich naturalnej rywalizacji. To samo tyczy się drugiego oczywistego aspektu ich aktywności zewnętrznej, czyli współpracy. Charakterystyka tego zagadnienia nie może się jednak oprzeć jedynie na prostym przeglądzie empirycznych przykładów tzw. cyberwojen, powinna natomiast ująć je zdecydowanie szerzej, w kontekście całokształtu zachowań podmiotów w środowisku międzynarodowym.

Główna hipoteza monografii zawiera się w stwierdzeniu, iż cyberprzestrzeń stała się nowym wymiarem polityki zagranicznej. Państwa w XXI wieku coraz częściej wykorzystują cyberataki, aby realizować swoje interesy w środowisku międzynarodowym, co implikuje zjawisko ich rywalizacji w przestrzeni teleinformatycznej. Ze względu na jej właściwości techniczne, otwartą architekturę, potencjał dla szeroko pojętej sfery informacyjnej czy brak obowiązujących regulacji prawno-politycznych, środki te jawią się jako dogodna i coraz skutecz-

niejsza metoda osiągania celów na arenie międzynarodowej. Rodzi to jednak zarazem poważne zagrożenia dla bezpieczeństwa państw, a szerzej: dla całego systemu międzynarodowego. Warunkuje to zatem również proces wzrastającej współpracy państw w zakresie bezpieczeństwa teleinformatycznego.

Na tej podstawie wysunięto następujące hipotezy robocze:

1. Rewolucja informatyczna oprócz niezaprzeczalnych korzyści przyniosła nowe zagrożenia dla bezpieczeństwa państw.
2. Cyberprzestrzeń ze względu na swoje unikalne właściwości stała się wymiarem, w którego ramach można stosować rozmaite instrumenty polityki zagranicznej.
3. Do najczęściej używanych środków należą: cyberterroryzm, cyberszpiegostwo oraz operacje zbrojne w cyberprzestrzeni. Unikalną rolę odgrywa także haktywizm patriotyczny, będący swoistym *quasi*-instrumentem.
4. Wykorzystanie cyberprzestrzeni przez państwa otwiera nowe możliwości realizowania interesów na arenie międzynarodowej. „Teleinformatyczne" instrumenty polityki zagranicznej pozwalają w niestandardowy sposób osiągać takie cele, jak zapewnienie bezpieczeństwa, wzrost potęgi (siły) oraz wzrost pozycji i prestiżu międzynarodowego. Ich skuteczność bywa jednak różna i mają one z reguły charakter komplementarny w stosunku do innych środków.
5. Ich zastosowanie przez poszczególne rządy determinuje zjawisko rywalizacji państw w cyberprzestrzeni.
6. Środki te stanowią zarazem nowy rodzaj zagrożeń dla bezpieczeństwa narodowego i międzynarodowego, są zatem również czynnikiem sprzyjającym zawiązywaniu współpracy państw w dziedzinie bezpieczeństwa teleinformatycznego.
7. Mimo że zakres kooperacji w cyberprzestrzeni w ostatnich latach stopniowo rośnie, nadal nie wypracowano w tej dziedzinie najpotrzebniejszych mechanizmów i rozwiązań.
8. W XXI wieku można odnotować przewagę rywalizacyjnej aktywności państw w cyberprzestrzeni nad aspektami koncyliacji i współpracy, co wiąże się z poważnymi konsekwencjami dla systemu międzynarodowego. Można tu wskazać na dwa najistotniejsze skutki: osłabienie efektywności prawa międzynarodowego oraz osłabienie skuteczności mechanizmów współpracy politycznej i wojskowej.

Głównym celem naukowym monografii jest więc wyjaśnienie, czy państwa rywalizują i współpracują w cyberprzestrzeni, czym się to przejawia oraz jakie są tego konsekwencje dla praktyki polityki zagranicznej oraz całokształtu stosunków międzynarodowych. Innymi słowy opracowanie to stara się odpowiedzieć na pytanie, czy działania w przestrzeni teleinformatycznej mogą być uznane za instrument polityki zagranicznej, zarówno w ujęciu rywalizacyjnym, jak i kooperacyjnym. Tego typu praktyka wiązałaby się bowiem z zasadniczymi

skutkami dla całego systemu międzynarodowego, nie tylko z perspektywy bezpieczeństwa.

Celem pracy jest również odpowiedź na szereg pytań badawczych, które powinny ułatwić realizację celu głównego:

1. Jakie były najważniejsze procesy i wydarzenia determinujące rewolucję informatyczną w XX i XXI wieku oraz jej podstawowe reperkusje dla funkcjonowania państw i społeczeństw?
2. Czym jest cyberprzestrzeń oraz jakie posiada właściwości z punktu widzenia jej przydatności dla czynników państwowych?
3. Czym są cyberataki oraz jakie są ich podstawowe metody w ujęciu technicznym?
4. Jakie są najpoważniejsze formy zagrożeń teleinformatycznych dla bezpieczeństwa państw z perspektywy nauki o stosunkach międzynarodowych?
5. Czy cyberataki można uznać za świadomy środek realizowania interesów państwa na arenie międzynarodowej? Jeśli tak, to jakie cele są w ten sposób realizowane oraz jaka jest ich skuteczność w porównaniu do zakładanych oczekiwań?
6. Czy rosnąca skala incydentów teleinformatycznych doprowadziła do nawiązania międzynarodowej współpracy w zakresie cyberbezpieczeństwa? Jeśli tak, to w jaki sposób się to przejawia oraz jaka jest skuteczność tej współpracy?
7. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na bezpieczeństwo międzynarodowe?
8. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na praktykę polityki zagranicznej?
9. Jaki jest wpływ rywalizacji i współpracy państw w cyberprzestrzeni na skuteczność prawa międzynarodowego i mechanizmów współpracy politycznej?

Aby zrealizować postawiony wyżej cel, odpowiedzieć na pytania badawcze oraz dokonać weryfikacji hipotezy głównej i hipotez roboczych, należałoby na wstępie wyjaśnić kilka kwestii. Przede wszystkim, o czym wspomniano już wyżej, problematyka szeroko pojętych konsekwencji szkodliwego wykorzystania technologii teleinformatycznych jest podejmowana nie tylko przez nauki społeczne, lecz również przez nauki techniczne i ścisłe. Podchodzą one do tych zagadnień odmiennie, co może czasami rodzić poważne spory terminologiczne i interpretacyjne. Każda z dziedzin wykształciła aparat pojęciowy (nie zawsze zresztą podzielany przez całe środowisko naukowe), skupiający się na właściwych jej zagadnieniach, który niekoniecznie musi być przydatny do analizy podobnych spraw z perspektywy innego obszaru wiedzy. W monografii zatem, bazując naturalnie na dotychczasowym dorobku nauk technicznych i ścisłych, podjęto badania z perspektywy stosunków międzynarodowych. Ma to określone konsekwencje dla stosowanych metod badawczych. Takie dyscypliny naukowe,

jak informatyka czy elektronika, operują z reguły bardzo konkretnymi, wyraźnie sprecyzowanymi kategoriami i pojęciami naukowymi. W ujęciu społecznym, na różnych poziomach analizy, tak z reguły nie jest. Na styku nowych technologii oraz czynnika ludzkiego, szczególnie w wymiarze politycznym i bezpieczeństwa, pojawiają się bowiem zjawiska dynamiczne, bardzo trudne do jednoznacznej oceny. Częstokroć poszczególne sposoby wykorzystania ICT nawzajem się przenikają i mają skutki na wielu pozornie niezwiązanych ze sobą płaszczyznach. Rodzi to oczywiste problemy dla metodologii badań nad aktywnością państw w cyberprzestrzeni. Jak bowiem wspomniano wcześniej, nie ma szeroko podzielanego konsensusu przedstawicieli nauk o polityce, nauk o bezpieczeństwie czy nauk o obronności co do stosowanej w tym zakresie siatki pojęciowej. W konsekwencji w literaturze specjalistycznej częstokroć używa się bardzo zróżnicowanej, a niekiedy mało sprecyzowanej nomenklatury naukowej. W związku z tym warunkiem *sine qua non* dokonania analizy rywalizacji i współpracy państw w cyberprzestrzeni powinno być zaproponowanie odpowiadającej stanowi faktycznemu terminologii w tym zakresie.

Ponadto powstaje pytanie, na jakim poziomie należałoby rozpatrywać postawiony problem badawczy. Jak pisał Edward Haliżak (2013a: 28), „wybór danego poziomu analizy wiąże się zawsze z przyjęciem określonych założeń ontologicznych" oraz „pełni ważną funkcję eksplanacyjną". W tym kontekście najbardziej właściwy wydaje się poziom polityki zagranicznej, rywalizację i współpracę państw w różnych wymiarach i płaszczyznach można bowiem uznać za konsekwencję realizacji odmiennych lub zbieżnych interesów i celów ich aktywności zewnętrznej. Odwołując się do rozważań Wojciecha Kosteckiego, wzięto pod uwagę dwa poziomy analizy polityki zagranicznej: państwowy oraz międzynarodowy. W pierwszym przypadku politykę zagraniczną „traktuje się jako rezultat krajowego splotu określonych czynników", w drugim natomiast „interpretowana jest jako reakcja na środowisko zewnętrzne" (Kostecki, 2012: 119), przy czym należy stwierdzić, że przyjęcie takiej optyki badawczej sprawia, iż formułowane wnioski dotyczą również wyższego poziomu — całego systemu międzynarodowego.

Analizując rywalizację i współpracę państw w nowej domenie, jaką jest cyberprzestrzeń, należałoby już na wstępie przyjąć określone definicje podstawowych terminów i kategorii z zakresu teorii polityki zagranicznej, które posłużą do rozważań w dalszych częściach pracy. Ze względu na fakt, iż kwestie te zostały już bardzo szeroko i wyczerpująco omówione w polskiej i zagranicznej literaturze specjalistycznej[3], nie ma sensu omawiać ich osobno w pierw-

[3] Zob. np.: Kukułka, 2003; Nowiak, 2000; Zięba, 2005a,b; Łoś-Nowak, 2008; Kostecki, 1988; Łoś-Nowak, 2011; Cziomer, 2005; Dobroczyński, Stefanowicz, 1984; Malendowski, Mojsiewicz, Czachór, Bryła, 2007; Holsti, 1967; Kondrakiewicz, 2013; Ociepka, 2013; Zając, 2005; Popiuk-Rysińska,1992; Bryła, 2000.

szym rozdziale pracy[4]. Przyjęto więc rozumienie polityki zagranicznej za Teresą Łoś-Nowak (2011: 47), która zauważyła, iż jest to „dynamiczny proces formułowania i realizacji interesów narodowych i celów polityki w poliarchicznym i policentrycznym środowisku międzynarodowym". Jeśli chodzi o cele polityki zagranicznej, kategorię o fundamentalnym znaczeniu dla realizacji celu badawczego, zdecydowano się na przyjęcie ich podziału za Ryszardem Zięba (2005a: 48—49), który wyróżnił cztery grupy celów: zapewnienie bezpieczeństwa państwa w stosunkach międzynarodowych, wzrost siły państwa, wzrost pozycji międzynarodowej i prestiżu oraz kształtowanie i optymalizacja reguł funkcjonowania środowiska międzynarodowego. Jeśli chodzi o pierwszą grupę celów, najpełniej oddał jej charakter Marian Dobrosielski (cyt. za: Malendowski, 2000: 386):

> przez zagwarantowanie bezpieczeństwa danego państwa rozumiemy dziś tworzenie takich warunków, które zapewniałyby mu istnienie własnej państwowości, suwerenności, integralność terytorialną, nieingerencję w sprawy wewnętrzne. Warunków, które umożliwiłyby rozwój osobowości i tożsamości narodowej, własnego języka, gospodarki, nauki i innych dziedzin życia. Chodzi więc o kształtowanie takiej sytuacji, która mogłaby zapewnić realizację celów, wartości, aspiracji danego państwa czy społeczeństwa, jego trwałych, żywotnych interesów.

Wzrost potęgi i siły Erhard Cziomer (2005: 131) określił jako wykorzystanie „wszelkich atutów wewnętrznych dla osiągania korzystnych efektów w kontaktach politycznych, gospodarczych, społecznych itp. z innymi państwami oraz uczestnikami stosunków międzynarodowych". Trzecia grupa celów zdaniem Ryszarda Zięby (2005a: 54) wyraża „koegzystencjalne interesy wyrastające z potrzeb: uczestnictwa w systemie międzynarodowym […], współpracy i współzawodnictwa z innymi państwami i narodami, potwierdzania suwerenności państwa i wzrostu jego roli międzynarodowej". Czwarta grupa celów polityki zagranicznej wywodzi się natomiast z wartości uniwersalnych, nie opiera się na egoizmie i dotyczy m.in. wsparcia międzynarodowego pokoju, umacniania systemu międzynarodowego, przeciwdziałania zagrożeniom dla bezpieczeństwa oraz rozwoju prawa i zwyczajów międzynarodowych (Ibidem, s. 56—68). W literaturze przedmiotu oprócz celów wyróżnia się jeszcze środki polityki zagranicznej, przez które można rozumieć „wszystkie zasoby i instrumenty, przy użyciu których państwa starają się kształtować pożądane postawy

[4] W pierwotnej wersji tej rozprawy pierwszy rozdział nosił tytuł *Pojęcie, uwarunkowania, cele i środki polityki zagranicznej.* Szeroko charakteryzował on dotychczasową dyskusję na ten temat, uwzględniając również wątki związane z rozumieniem rozmaitych kategorii związanych z bezpieczeństwem. Ze względu jednak na słuszną uwagę Recenzenta, iż sprawy te zostały już wielokrotnie omówione w literaturze specjalistycznej, zdecydowano się na jego usunięcie.

i działania zagranicznych podmiotów oraz pożądane stany zjawisk i procesów międzynarodowych”[5].

Na tym tle, należałoby również wyjaśnić, czym jest rywalizacja i współpraca państw. W pracy przyjęto rozumienie rywalizacji za Agatą Włodowską-Bagan (2012: 105, 111)[6], według której

> Dokonując pewnego uogólnienia, można […] wskazać dwa elementy, które wydają się niezbędne dla uznania stosunków między państwami za rywalizację. Po pierwsze, chodzi o […] sprzeczność interesów, wynikającą z jednoczesnego ubiegania się o pierwszeństwo lub zdobycie czegoś lub kogoś, a po drugie o czynnik psychologiczny związany z identyfikacją państwa jako rywala. […] Należy dokonać tu wyraźnego rozróżnienia, jako że nie każdy konflikt jest rywalizacją i nie w każdej rywalizacji mamy do czynienia z użyciem siły. Rywalizacja, choć może być przyczyną konfliktów, nie jest jednak niezbędna do ich powstawania.

Z kolei współpracę państw trafnie wyjaśnił Robert Koehan, który stwierdził, iż „ma [ona — M.L.] miejsce wtedy, gdy uczestnicy dostosowują swoje zachowanie do aktualnych i oczekiwanych preferencji innych uczestników poprzez proces koordynacji działań” (cyt. za: Haliżak, 2006: 236).

Oprócz podstawowych pojęć i klasyfikacji z zakresu teorii polityki zagranicznej ze względu na podejmowaną w rozprawie problematykę należałoby we wstępie także wyjaśnić, co rozumie się przez bardzo pojemny termin, jakim jest *bezpieczeństwo*[7]. Definicję bezpieczeństwa narodowego przyjęto zatem za Waldemarem Kitlerem (2002: 48), który rozumiał przez to proces obejmujący zabiegi (np. politykę zagraniczną, przedsięwzięcia ochronne i obronne), których celem jest stworzenie korzystnych warunków funkcjonowania państwa na „arenie międzynarodowej oraz wewnętrznej oraz przeciwstawienie się wyzwaniom i zagrożeniom bezpieczeństwa”. Z kolei bezpieczeństwo międzynarodowe zgodnie z interpretacją Romana Kuźniara (2012a: 15) uznano za „brak zagrożeń dla norm, reguł i instytucji, które służą zapewnianiu bezpieczeństwa państw i pozostałych uczestników stosunków międzynarodowych”. Należy przy tym zaznaczyć, że oba te pojęcia są uznawane obecnie za nieostre, co wynika m.in. z coraz

[5] Rozróżnia się środki polityczne, ekonomiczne, wojskowe, kulturowo-ideologiczne oraz inne. Oprócz nich funkcjonuje pojęcie metod polityki zagranicznej, przez które Justyna Zając (2005: 79—80) rozumie „sposoby posługiwania się przez państwa środkami. Metody te można podzielić na: pozytywne, czyli nakłanianie; negatywne, czyli przymus, oraz neutralne”.

[6] Zob. także Sułek, 2012: 35—49.

[7] Zob. np.: Kowalkowski, 2011; Zięba, 2011; Czaputowicz, 2006, 2012; Kołodziej, 1997; Pietraś, 2000; Kuźniar, 2006a,b; Kukułka, 1995; Baldwin, 1997; Bobrow, 1997; Cziomer, 2005; Kuźniar, Balcerowicz, Bieńczyk-Missala, Grzebyk, Madej, Pronińska, Sułek, Tabor, Wojciuk, 2012; Wolfers, 1952; Kuźniar, 2012a,b; Herz, 1959; Madej, 2005; Kitler, 2002; Gała, 2009; Łebkowska, 2011; Mojsiewicz, 2000.

szerszej gamy determinantów wpływających w okresie pozimnowojennym na bezpieczeństwo państw. Jak stwierdził Marek Madej (2005: 491):

> stopniowo krystalizuje się współczesne pojmowanie bezpieczeństwa, bardziej systemowe, całościowe i wszechstronne (tzn. obejmujące możliwie najpełniejsze spektrum zagadnień i sfer życia społecznego, na których mogą powstawać problemy bezpieczeństwa). Takie ujęcie (czy też ujęcia, nie można bowiem w tym przypadku mówić o jednym, dominującym modelu) lepiej odpowiada obecnemu kształtowi stosunków międzynarodowych, w których relacje między poszczególnymi ich uczestnikami dalece odbiegają […] od względnej jednoznaczności okresu zimnowojennego.

W związku z tym w ujęciu przedmiotowym (Kukułka, 1994: 40—41) wyróżnia się już nie tylko bezpieczeństwo polityczne (Pawlikowska, 2005: 62) i wojskowe (Balcerowicz, 2005: 478—481; Nowak, Nowak, 2011: 72; Żukrowska, 2006: 32), lecz także gospodarcze (ekonomiczne) (Haliżak, 1997: 78; Anokhin, Grishin, 2013: 155—163), ekologiczne (Pietraś, 2000: 20) czy społeczno-kulturowe (Czaputowicz, 2006: 75; Leszczyński, 2011; Michałowska, 1997; Lizak, 1997; Zakrzewski S., 2013: 165—174).

Od pewnego czasu coraz częściej dodaje się do tej listy jeszcze jeden, kluczowy dla dalszych rozważań, wymiar przedmiotowy bezpieczeństwa. Jak pisali Agnieszka Bógdał-Brzezińska i Marcin Florian Gawrycki (2003: 40—41):

> wraz z postępem technologicznym i cywilizacyjnym sfera bezpieczeństwa publicznego rozszerzyła się na nowe dziedziny. Współczesne pojęcie bezpieczeństwa informacyjnego lub cybernetycznego (*cybersecurity*) odnosi się zatem do stosunkowo młodej, ale bardzo prężnie rozwijającej się i bardzo wrażliwej sfery ICT. Jest ona zarówno obszarem prywatnej aktywności obywateli, jak też strategicznym czynnikiem rozwoju gospodarki narodowej (cyberekonomia).

W związku z tym, zdaniem autorów, „bezpieczeństwo informacyjne (BI) funkcjonuje w powiązaniu z szeregiem tradycyjnych wymiarów bezpieczeństwa państwa" (Ibidem). W tym kontekście część badaczy, omawiając te zagadnienia, pisze o bezpieczeństwie informacyjnym rozumianym często jako „ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania" (Liedel, 2011: 56—57). W literaturze specjalistycznej przyjmuje się jednak często inne podejście, zakładające skupienie się wyłącznie na problematyce związanej z technologiami teleinformatycznymi[8], a nie szerszą kategorią infor-

[8] Józef Janczak oraz Andrzej Nowak (2013: 20—21) stwierdzili, że bezpieczeństwo informacyjne jest pojęciem bardzo szerokim i można je podzielić na dwa rodzaje: bezpieczeństwo informacji (ochrona wszystkich form wymiany, przechowywania i przetwarzania danych) oraz bezpieczeństwo teleinformatyczne.

macji[9]. Wobec tego ujęcie to określa się z reguły mianem *bezpieczeństwa teleinformatycznego* lub *cyberbezpieczeństwa*. Można przez to rozumieć za Markiem Madejem i Marcinem Terlikowskim (2009: 10—11)

> zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej bez jego zgody i wiedzy, wszelkiego rodzaju informacji utrwalonej w postaci cyfrowej oraz możliwość jej bezpiecznego (tzn. nienarażonego na przechwycenie, zniszczenie lub nieuprawnioną modyfikację) przetwarzania, przesyłania i upowszechniania[10].

Znając znaczenie podstawowych terminów wykorzystywanych w dalszych częściach pracy, warto odnieść się wreszcie do pewnych wątpliwości związanych z dostępnością faktografii. Analiza aktywności państw w cyberprzestrzeni rodzi bowiem zasadnicze trudności, wynikające z obiektywnych właściwości tej domeny. Jej charakter sprawia, iż jednoznaczna identyfikacja pośrednich i bezpośrednich sprawców cyberataków bywa bardzo trudnym, a czasami wręcz niemożliwym zadaniem. W przeciwieństwie do badań skupiających się na wydarzeniach politycznych, gospodarczych czy wojskowych ustalenie faktów związanych z działaniami w sieciach komputerowych jest o wiele bardziej skomplikowane. W związku z tym przyjęto tu kilka rozwiązań. Przede wszystkim bez względu na fakt, iż jest to praca z dziedziny nauk społecznych, oparto się bardzo szeroko na analizach przeprowadzonych przez przedstawicieli nauk ścisłych i technicznych. Szczególnie przydatne do omówienia przypadków rywalizacji państw w przestrzeni teleinformatycznej okazały się opracowania czołowych korporacji zajmujących się zabezpieczeniami komputerowymi czy zwalczaniem złośliwego oprogramowania (np. Symantec, McAfee czy Kaspersky Lab). Bardzo często w toku prowadzonych przez nie badań natrafiano na wskazówki lub dowody pozwalające na identyfikację osób bądź podmiotów odpowiedzialnych za dane włamanie. Podobne osiągnięcia odnotowało wiele zespołów naukowców lub ośrodków analizujących zagrożenia dla bezpieczeństwa teleinformatycznego, takich jak np.

---

[9] Krzysztof Liedel (2011: 56—57) zauważył, iż informacja stanowi w XXI wieku zasób strategiczny, wynikająca z niej wiedza i technologie stają się podstawowym czynnikiem wytwórczym, dochody państwa w coraz większym stopniu będą uzyskiwane dzięki sektorowi informacyjnemu, procesy decyzyjne w innych sektorach gospodarki i życia społecznego będą uzależnione od systemów przetwarzania i przesyłania informacji, ich zakłócenie nie wymaga wielkich nakładów, a rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej. Z kolei Krzysztof Liderman (2009: 10) uznał, że informacja „była, jest i będzie towarem. Informacje mają jednak tę szczególną właściwość, odróżniającą je od innych towarów (przedmiotów materialnych, usług), że aby udzielić ich jednym (osobom), wcale nie trzeba odbierać ich innym".

[10] W tym kontekście mówi się też często o swoistej triadzie bezpieczeństwa teleinformatycznego, w której skład wchodzą integralność, poufność oraz dostępność informacji. Zob. Madej, Terlikowski, 2009: 10—11.

kanadyjski Citizen Lab. Na tej podstawie starano się wskazać, czy istniała korelacja między motywami, celami polityki zagranicznej poszczególnych państw a incydentami teleinformatycznymi. Jeśli taki związek istniał, był to kolejny argument pozwalający na przyjęcie określonej interpretacji wydarzeń. Wreszcie sprawdzano, czy ataki komputerowe wpisywały się w specyfikę całokształtu stosunków dwu- lub wielostronnych i jaką odgrywały w nich potencjalnie rolę.

Wszystkie powyższe założenia wymagały więc zastosowania szeregu metod badawczych właściwych dla nauk społecznych. Przede wszystkim wykorzystano metodę analizy historycznej, przydatnej do omówienia przebiegu i globalnych skutków rewolucji informatycznej w XX i XXI wieku. Odpowiedź na pytanie, jak w przeszłości ewoluowały technologie informacyjne i komunikacyjne, miała fundamentalne znaczenie dla zrozumienia fenomenu cyberprzestrzeni jako nowej domeny rywalizacji i współpracy państw. Po drugie — odwołano się do metody analizy treści m.in. oficjalnych dokumentów, wypowiedzi polityków bądź opinii analityków. Jak wspomniano bowiem wyżej, od niemal trzech dekad trwa bardzo ożywiona debata na temat konsekwencji szkodliwego wykorzystania technologii informatycznych. Charakterystyka tych zagadnień bez znajomości najnowszych trendów i wniosków z tej dyskusji nie byłaby więc możliwa. Po trzecie — w rozdziałach dotyczących empirycznych przykładów rywalizacji i współpracy odwołano się do metody analizy decyzyjnej oraz analizy instytucjonalno-prawnej. Metoda decyzyjna pomogła w wyjaśnieniu zjawisk międzynarodowych na podstawie konkretnych decyzji politycznych. Kluczowe było tu wskazanie nie tylko powodów podjęcia danej decyzji, ale także jej wpływu na całokształt rzeczywistości międzynarodowej. Z kolei metoda instytucjonalno-prawna, polegająca na badaniu aktów normatywnych, była szczególnie przydatna przy analizie przejawów współpracy rządów w tej dziedzinie. Po czwarte — zastosowano metodę komparatywną dla porównania, w jaki sposób poszczególne podmioty wykorzystywały potencjał sieci teleinformatycznych do realizacji określonych celów w środowisku międzynarodowym. Po piąte — aby zrozumieć globalny charakter zagrożeń teleinformatycznych oraz ich wpływ na stosunki międzynarodowe, użyto metod ilościowych (statystycznych), polegających na zebraniu i przetworzeniu masowych informacji o niekorzystnych trendach w cyberprzestrzeni. Odwołano się ponadto do kilku podstawowych metod badawczych, takich jak analiza i krytyka źródeł, analiza i krytyka piśmiennictwa, metoda obserwacji faktów oraz synteza i opis*.

Struktura pracy ma charakter problemowy. W rozdziale pierwszym przedstawiono główne etapy, istotę i konsekwencje rewolucji informatycznej. Omówienie tych zagadnień było o tyle ważne, iż stanowiło podstawowy warunek

* W pierwotnej wersji pracy zastosowano przypisy dolne. W procesie wydawniczym, ze względu na znaczną ich liczbę oraz związane z tym wątpliwości co do czytelności monografii, zdecydowano o zastosowaniu zmodyfikowanego systemu harwardzkiego. Jednocześnie ze względu na specyfikę pracy pozostawiono w przypisach dolnych liczne źródła internetowe.

zrozumienia potencjału technologii teleinformatycznych oraz ich wpływu na funkcjonowanie człowieka i jego zbiorowości. W tym kontekście scharakteryzowano główne osiągnięcia i odkrycia poczynione w XX i XXI wieku, zarówno z dziedzinie telekomunikacji, jak i informatyki. Szczególny nacisk położono na proces powstawania sieci komputerowych oraz wynikających z tego implikacji dla najważniejszych obszarów życia ludzkiego, w tym komunikacji, polityki, kultury, gospodarki czy życia społecznego.

Na tej podstawie w rozdziale drugim omówiono, czym jest cyberprzestrzeń[11] oraz z jakimi konsekwencjami wiąże się jej funkcjonowanie. Przede wszystkim scharakteryzowano wieloletnią debatę poświęconą temu pojęciu, konfrontując się zarówno z jego zwolennikami, jak i przeciwnikami. Następnie przyjęto własną interpretację znaczenia tego terminu, co było warunkiem przejścia do dalszych etapów badań. Omówiono ponadto główne właściwości techniczne cyberprzestrzeni, w tym wielowarstwowy, wielopodmiotowy charakter związany z otwartą architekturą czy promieniowaniem elektromagnetycznym. Wskazano również na jej najważniejsze cechy jako nowego wymiaru bezpieczeństwa narodowego i międzynarodowego. Tym samym przedstawiono powody, dla których przestrzeń teleinformatyczna stała się interesującą i unikalną sferą realizacji interesów i celów polityki zagranicznej. Scharakteryzowano także pokrótce ewolucję szkodliwej aktywności w sieciach komputerowych, począwszy od lat 60. XX wieku, współczesną skalę oraz konsekwencje o zasięgu globalnym.

W rozdziale trzecim podjęto próbę sformułowania podstawowej siatki pojęciowej dotyczącej zagrożeń dla bezpieczeństwa teleinformatycznego w oparciu o wcześniejsze rozważania oraz wieloletnią debatę naukową na ten temat. Niezbędna dla zrozumienia aktywności państw w cyberprzestrzeni analiza tych wyzwań wyszła od wskazania głównych podmiotów odpowiedzialnych za szkodliwą działalność w sieci. Wzięto tu pod uwagę dwa czynniki: stopień organizacji sprawców oraz ich motywacje. Zdefiniowano również, czym są cyberataki oraz jakie są ich główne metody w ujęciu technicznym. Na tej podstawie skonstruowano uproszczoną typologię zagrożeń teleinformatycznych, do których zaliczono haking, haktywizm, cyberprzestępczość, haktywizm patriotyczny, cyberszpiegostwo, cyberterroryzm oraz operacje zbrojne w cyberprzestrzeni. Scharakteryzowano ponadto kontrowersyjne zjawisko cyberwojny, odnosząc się zarówno do krytyków, jak i zwolenników stosowania tej kategorii.

Rozdział czwarty został poświęcony analizie empirycznych przykładów rywalizacji państw w cyberprzestrzeni oraz wynikających z tego konsekwencji dla ich bezpieczeństwa oraz polityki zagranicznej. Do analizy wybrano osiem najlepiej udokumentowanych oraz najbardziej znanych przykładów: stosunki na linii Rosja — Estonia, Rosja — Litwa, Rosja — Gruzja, Rosja — Kirgistan,

[11] W pracy używano także synonimów: *przestrzeń teleinformatyczna*, *środowisko teleinformatyczne*.

Izrael — Syria, Izrael — USA — Iran, USA — Chiny oraz Korea Północna — Korea Południowa[12]. W badaniu brano pod uwagę przede wszystkim uwarunkowania stosunków dwu- lub wielostronnych oraz interesy i cele formułowane przez wszystkie zainteresowane strony. Dalej omawiano przebieg i specyfikę incydentów teleinformatycznych oraz ich wpływ na bezpieczeństwo zaatakowanych podmiotów. Na tej podstawie dokonywano próby określenia, czy cyberataki rzeczywiście zostały wykorzystane w charakterze nowego, unikalnego środka polityki zagranicznej. Jeśli odpowiedź była twierdząca, starano się zidentyfikować cele, które w ten sposób realizowano, oraz skuteczność takich przedsięwzięć.

W rozdziale ostatnim przedstawiono natomiast cyberprzestrzeń jako nowy wymiar współpracy państw. Omówiono tu powody, dzięki którym społeczność międzynarodowa w coraz większym stopniu wykazuje chęć kooperacji w tym zakresie. Scharakteryzowano ponadto globalną debatę, która od lat toczy się w łonie Organizacji Narodów Zjednoczonych, m.in. nad zjawiskiem cyberprzestępczości, cyberwojny czy nieskutecznością prawa międzynarodowego. Wskazano także na unikalny *casus* Międzynarodowego Związku Telekomunikacyjnego, będącego organizacją, która wypracowała jak dotąd najskuteczniejsze mechanizmy praktycznej współpracy w tej dziedzinie. Omówiono również najbardziej zaawansowane przedsięwzięcia podejmowane na szczeblu regionalnym na przykładzie Paktu Północnoatlantyckiego oraz Unii Europejskiej oraz przedstawiono aktywność w tej sferze kilku innych organizacji międzynarodowych, takich jak Rada Europy, Unia Afrykańska czy Organizacja Współpracy Gospodarczej i Rozwoju[13]. Na tej podstawie spróbowano odpowiedzieć na pytanie, jaka jest skuteczność tego typu środków w świetle oczekiwanych przez państwa członkowskie rezultatów współpracy na arenie międzynarodowej.

Temat monografii nie doczekał się dotychczas zwartego opracowania w polskiej i zagranicznej literaturze naukowej. Od końca XX wieku coraz częściej pojawiają się ciekawe prace naukowe poświęcone szkodliwemu wykorzystaniu cyberprzestrzeni. Zdecydowana większość publikacji na ten temat zawęża jednak problematykę badawczą wyłącznie do aspektów związanych z bezpie-

[12] Oczywiście nie zamyka to listy wszystkich znanych opinii publicznej incydentów teleinformatycznych, których stronami były państwa. Wybrane przykłady spotkały się jednak z największym zainteresowaniem badaczy oraz były przedmiotem pogłębionych analiz zarówno z perspektywy nauk społecznych, jak i technicznych. Nie podjęto więc w pracy tych wątków, które nie zostały w wyczerpujący sposób omówione przez ekspertów z zakresu informatyki bądź ich znaczenie dla omawianego tematu jest nikłe. Chodzi tu m.in. o takie przypadki, jak rola cyberataków w stosunkach indyjsko-pakistańskich czy izraelsko-palestyńskich.

[13] Klucz doboru oparto na dwóch przesłankach. Po pierwsze: celem było wyeksponowanie dorobku kilku organizacji rządowych mających relatywnie duże znaczenie w systemie stosunków międzynarodowych. Po drugie: zaprezentowano podmioty, które przyjmowały możliwie jak najbardziej zróżnicowane podejście do tematyki cyberbezpieczeństwa, odnosząc w tym wymiarze zarówno sukcesy, jak i ponosząc spektakularne porażki. Pozwoliło to na zobrazowanie szerokiego spektrum przedsięwzięć w tej dziedzinie.

czeństwem teleinformatycznym, zarówno w ujęciu politologicznym, jak i prawnym, technicznym bądź wojskowym. Z reguły bardzo skrótowo podejmuje się natomiast wątki szerszych konsekwencji aktywności państw w sieci na poziomie narodowym i międzynarodowym. Bez względu na ten fakt w pracy wykorzystano bogatą literaturę polsko-, anglo- oraz francuskojęzyczną. Jeśli chodzi o polskie opracowania, to nie sposób wymienić wszystkich autorów, których dzieła pomogły w analizie zjawiska rywalizacji i współpracy państw w cyberprzestrzeni. Warto jednak wymienić tych, których monografie bądź artykuły okazały się najbardziej przydatne: Piotr Sienkiewicz, Marek Madej, Marcin Terlikowski, Marcin Florian Gawrycki, Agnieszka Bógdał-Brzezińska, Krzysztof Liedel, Paulina Piasecka, Krzysztof Liderman oraz Ernest Lichocki. Piotr Sienkiewicz jest uznawany za jeden z największych krajowych autorytetów, jeśli chodzi o takie zagadnienia, jak wojna i walka informacyjna, cyberbezpieczeństwo, a także dowodzenie, cybernetyka czy inżynieria systemów (zob. Goban-Klas, Sienkiewicz, 1999; Sienkiewicz, 2003; Sienkiewicz, Świeboda, 2006, 2009). Marek Madej i Marcin Terlikowski są redaktorami jednej z najciekawszych prac zbiorowych poświęconych bezpieczeństwu teleinformatycznemu państw oraz autorami interesujących publikacji na ten temat (Madej, Terlikowski, red., 2009; Terlikowski, Rękawek, Kozłowski, 2014). Marcin Florian Gawrycki oraz Agnieszka Bógdał-Brzezińska w wielu swoich publikacjach nie tylko wnikliwie scharakteryzowali zjawisko cyberterroryzmu, ale także inne niekorzystne konsekwencje rewolucji informatycznej (Bógdał-Brzezińska, Gawrycki, 2003, 2004; Bógdał-Brzezińska, 2009). Krzysztof Liedel oraz Paulina Piasecka są z kolei uznanymi autorami wielu przydatnych prac z zakresu szeroko pojętego bezpieczeństwa informacyjnego, w tym np. fenomenu cyberwojny (Piasecka, 2011; Liedel, 2011; Liedel, Piasecka, 2011; Liedel, Piasecka, Aleksandrowicz, red., 2014). Warto również wspomnieć o publikacjach Krzysztofa Lidermana (2009, 2012) oraz Ernesta Lichockiego (2008, 2011). Pierwszy z nich przygotował interesujące opracowania dotyczące bezpieczeństwa informacyjnego, drugi natomiast specjalizuje się od lat w tematyce cyberterroryzmu.

Wśród literatury anglojęzycznej za najbardziej wartościowe należy uznać m.in. publikacje: Ronalda Deiberta, Rafała Rohozinskiego, Martina C. Libickiego, Patricka Hessa, Jamesa A. Lewisa, Jeffreya Carra, Johna V. Blane'a, Thomasa Rida, Richarda A. Clarke'a oraz Roberta K. Knake'a. Ron Deibert oraz Rafał Rohozinski od lat są czołowymi kanadyjskimi badaczami zajmującymi się szeroko pojętym bezpieczeństwem teleinformatycznym. Nie tylko sami są autorami wielu publikacji na ten temat, ale także prowadzone przez nich zespoły i ośrodki badawcze wsławiły się przełomowymi odkryciami w tej dziedzinie (np. chińskiej siatki szpiegowskiej *Gh0stNet*) (Deibert, 2013; Deibert, Rohozinski, 2009, 2010). Nie mniejszym uznaniem cieszy się Martin C. Libicki z RAND Corporation, który opublikował wiele opracowań dotyczących m.in. zjawiska cyberwojny czy bezpieczeństwa informacyjnego (Libicki, 2007, 2013; Dziwisz, 2013). Za bardzo

przydatne należy uznać również raporty przygotowywane przez Jamesa A. Lewisa oraz Jeffreya Carra, będących jednymi z najczęściej cytowanych amerykańskich specjalistów zajmujących się analizą incydentów komputerowych (Lewis, 2002, 2006, 2010, 2012; Carr, Rios, Plansky i in., 2009). Patrick Hess (2001) i John V. Blane (2001) zasłynęli z kolei dwoma stosunkowo dawno już opublikowanymi, lecz nadal aktualnymi opracowaniami dotyczącymi cyberterroryzmu. Nie można także pominąć Thomasa Rida (2012: 5—32; 2013), który w ostatnich latach stał się jednym z najgłośniejszych krytyków terminu *cyberwojny*. Należy ponadto wspomnieć o budzącej kontrowersje, choć zarazem bardzo przydatnej publikacji byłego doradcy prezydentów Billa Clintona i George'a W. Busha — Richarda A. Clarke'a (Clarke, Knake, 2010). Jeśli chodzi natomiast o autorów frankofońskich, to można wymienić przede wszystkim Jeana Guisnela (1997b), Limore Yagil (2002) oraz Alessandro Buffaliniego (2012).

W monografii szeroko wykorzystano opracowania opublikowane w czołowych polskich i międzynarodowych czasopismach naukowych zajmujących się m.in. bezpieczeństwem, prawem, informatyką oraz stosunkami międzynarodowymi. Wśród rodzimych periodyków, które okazały się przydatne, należy wymienić m.in.: „Stosunki Międzynarodowe — International Relations", „Bezpieczeństwo Narodowe", „Przegląd Zachodni", „Przegląd Strategiczny" czy „Sprawy Międzynarodowe". Jeśli chodzi zaś o zagraniczne, nie można pominąć takich pozycji, jak: „International Security", „Journal of Strategic Studies", „Journal of Strategic Security", „Berkeley Journal of International Law", „The Journal of International Policy Solutions", „Journal of Systemics, Cybernetics and Informatics", „International Journal of Technoethics" czy „Journal of Computers".

Praca została ponadto oparta na licznych dokumentach źródłowych, statystykach, raportach, strategiach oraz opracowaniach wydanych przez organizacje międzynarodowe (w tym Organizację Narodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny, Sojusz Północnoatlantycki, Unię Europejską, Radę Europy czy Unię Afrykańską), instytucje i organy poszczególnych państw (koncepcje polityki zagranicznej, strategie wojskowe, strategie cyberbezpieczeństwa), ośrodki badawcze z całego świata (np. RAND Corporation, Center for a New American Century, Belfer Center for Science and International Affairs, Center for Strategic and International Studies, Chatham House, Citizen Lab), a także czołowe korporacje szeroko pojętego sektora IT (McAfee, Microsoft, Symantec, Kaspersky Lab). W pracy szeroko czerpano także, co naturalne, z danych i materiałów zamieszczanych w Internecie, przede wszystkim na portalach specjalistycznych, zajmujących się bezpieczeństwem teleinformatycznym (np. „Wired", Niebezpiecznik.pl, ZDNet). W uzasadnionych wypadkach korzystano również z witryn najważniejszych na świecie ośrodków medialnych, takich jak BBC, „The Guardian", „The New York Times" czy „The Washington Post".

Kończąc, chciałbym serdecznie podziękować wszystkim osobom, dzięki którym przygotowanie tej monografii było możliwe: przede wszystkim mojemu wieloletniemu opiekunowi naukowemu, profesorowi Mieczysławowi Stolarczykowi, kierownikowi Zakładu Stosunków Międzynarodowych w Instytucie Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego. Jego celne uwagi i wskazówki stanowiły ogromną pomoc na każdym etapie prac nad tą książką. Chciałbym również podziękować recenzentowi wydawniczemu publikacji, profesorowi Michałowi Chorośnickiemu, kierownikowi Katedry Teorii i Strategii Stosunków Międzynarodowych w Instytucie Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Jagiellońskiego. Jego cenne sugestie pozwoliły znacząco podnieść poziom merytoryczny prezentowanej monografii. Za pomoc dziękuję także Andrzejowi Kędzierskiemu, kierownikowi Sekcji Informatycznej Sądu Rejonowego w Będzinie, który zgodził się pełnić rolę konsultanta technicznego, dzięki czemu udało się wyeliminować szereg błędów i nieścisłości z pierwotnej wersji tej rozprawy. Wyrazy wdzięczności kieruję także w stronę International Council for Canadian Studies, dzięki któremu w 2011 roku byłem w stanie zrealizować grant naukowy poświęcony cyberbezpieczeństwu Kanady. Zdobyte podczas pobytu w Toronto doświadczenia okazały się bardzo przydatne w badaniach nad rywalizacją i współpracą państw w cyberprzestrzeni. Serdecznie dziękuję również władzom Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego oraz Wydziału Nauk Społecznych Uniwersytetu Śląskiego za wyasygnowanie środków, dzięki którym publikacja ta mogła ukazać się w druku.

Rozdział 1

Rewolucja informatyczna

1.1. Źródła rewolucji informatycznej

Drogę bezprecedensowego rozwoju naukowo-technicznego, na którą ludzkość wkroczyła po drugiej wojnie światowej, należy uznać za zjawisko wyjątkowe, zarówno ze względu na skalę, jak i doniosłe konsekwencje. Procesy komputeryzacji, informatyzacji oraz pojawienie się sieci Internet na całym świecie otworzyły nowe, niespotykane wcześniej możliwości przetwarzania, przechowywania i przesyłania informacji w różnej formie. Proliferacja technologii informacyjnych i komunikacyjnych (ICT), obejmując w drugiej połowie XX wieku niemal wszystkie sfery życia człowieka, doprowadziła w konsekwencji do zasadniczych zmian w wymiarze społecznym, kulturowym, gospodarczym, a nawet politycznym. W XXI wieku stały się one widoczne w rozmaitych płaszczyznach, począwszy od jednostek i najmniejszych struktur społecznych, aż po procesy o zasięgu globalnym. W opinii wielu badaczy nowe technologie stały się więc szansą, aby wprowadzić ludzkość w nową erę, wolną od problemów znanych z XIX i XX wieku. Zdaniem innych jednak wraz z niewątpliwymi korzyściami pojawiły się nowe, nieznane wyzwania. Te najistotniejsze dotyczą wymiaru egzystencjalnego, czyli bezpieczeństwa, osiągnięcia teleinformatyki stały się bowiem narzędziami wykorzystywanymi powszechnie, nie tylko przez pojedynczych użytkowników, ale przede wszystkim w wielu dziedzinach funkcjonowania państw i społeczeństw. Poszczególne rządy stosunkowo szybko dostrzegły ogromne korzyści wynikające z ich stosowania zarówno w wymiarze wewnętrznym, jak i międzynarodowym. Zbyt późno zdano sobie jednak sprawę, że wraz z coraz większym uzależnieniem od nowych technologii struktury państwowe, a co za tym idzie również obywatele stają się swoistymi zakładnikami

ich niezawodności. W tym kontekście wydaje się, iż analiza rewolucji informatycznej[1], jej najistotniejszych cech i konsekwencji, ma zasadnicze znaczenie dla realizacji postawionego we wstępie celu badawczego. Przede wszystkim pozwoli to pełniej zrozumieć charakter nowych technologii, a dzięki temu istotę cyberprzestrzeni oraz jej właściwości zarówno z perspektywy nauk technicznych, jak i społecznych. Po drugie natomiast przyczyni się to w znacznym stopniu do zrozumienia skali nowych zagrożeń dla różnych obszarów bezpieczeństwa państw, wynikających z powszechnego zastosowania osiągnięć teleinformatyki.

Badając to niezwykle skomplikowane i wielopłaszczyznowe zagadnienie, warto na wstępie podkreślić, iż postęp technologiczny zawsze implikował szeroko pojęte skutki społeczne. W przeszłości rewolucja rolnicza, rozwój zdolności obróbki metali, wynalezienie maszyny drukarskiej czy rewolucja przemysłowa (zob. np. Toffler, 1980) wiązały się z doniosłymi przemianami kulturowymi, gospodarczymi, społecznymi czy wreszcie politycznymi. Na tym tle należy zauważyć, iż już po drugiej wojnie światowej wielu badaczy zaczęło dostrzegać pierwsze symptomy świadczące o początku nowej ery rozwoju technologicznego ludzkości, która była jakościowo odmienna od wcześniejszych etapów. Przykładowo Kenneth E. Boulding w 1953 roku pisał o rewolucji organizacyjnej, której jedną z cech była wzrastająca rola dużych organizacji gospodarczych. Ralf Dahrendorf pod koniec lat 50. XX wieku odnotował początki społeczeństwa postkapitalistycznego (za: Giddens, 1975: 53—59). Daniel Bell wskazywał w latach 60. i 70. na koniec „ery ideologii" oraz powstanie „społeczeństwa postindustrialnego". Główną cechą tych przemian miało być z jednej strony zdezaktualizowanie się dotychczasowych ideologii XIX- i XX-wiecznych, z drugiej natomiast oparcie życia ludzkiego na informacji oraz usługach (Bell, 1960, 1999). Prorocza okazała się wizja Marshalla McLuhana (2003), który w połowie lat 60. omówił proces powstawania „globalnej wioski", co według niego wynikało przede wszystkim z dynamicznego rozwoju technologii informacyjnych (zob. też McLuhan, Fiore, 1968). W tym kontekście widać więc wyraźnie, iż duża grupa badaczy już w połowie XX wieku dostrzegała wielopłaszczyznowe procesy, które miały w przyszłości doprowadzić do przełomowych zmian we wszystkich sferach życia człowieka. Współcześnie w literaturze specjalistycznej określa się je najczęściej mianem *rewolucji informacyjnej* lub *rewolucji informatycznej*.

[1] Warto pamiętać, iż zdaniem Myriam Dunn-Cavelty (2008: 15) rewolucja z reguły oznacza radykalną, kompletną i natychmiastową zmianę. W tym kontekście zadała ona pytanie, czy rzeczywiście zmiany technologiczne po II wojnie światowej miały te cechy. Zdaniem autorki zdecydowanie właściwsze do charakterystyki tych zagadnień byłoby więc słowo *ewolucja*. Na problem ten można jednak spojrzeć nieco szerzej i ujmować go w kontekście całokształtu dziejów ludzkości. Wówczas okres proliferacji technologii ICT oraz dokonane przez nie zmiany rzeczywiście mogą być postrzegane jako rewolucja. Zob. też: Szpunar, 2012: 15.

Należy zauważyć, iż wbrew pozorom nie są to pojęcia w pełni tożsame. *Rewolucja informacyjna* jest terminem dość szeroko i interdyscyplinarnie ujmującym procesy, które rozpoczęły się po drugiej wojnie światowej. Wynika to przede wszystkim z samej definicji *informacji*, która bywa rozumiana bardzo różnie. Zbigniew Messner uznał ją za dane o procesach i zjawiskach gospodarczych, które mogą być wykorzystane w procesach podejmowania decyzji (Messner, 1971, cyt. za: Myszczyn, Myszczyn, 2003: 134). Według Piotra Sienkiewicza jest to „zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne" (cyt. za: Liedel, 2011: 50—51). W ujęciu Czesława Bermana można ją rozumieć w czterech znaczeniach: rzeczy, wielkości mierzalnej, potencjału i zmiany (Ibidem, s. 50—51). Norbert Wiener zdefiniował *informację* jako nazwę opisującą „treść zaczerpniętą ze świata zewnętrznego w procesie naszego dostosowania się do niego i przystosowania się do niego naszych zmysłów" (cyt. za: Stefanowicz, 2013: 8). W opinii Glynna Harmona jest to „metaenergia — impuls energetyczny, który reguluje większe ilości energii w różnych rodzajach systemów biologicznych lub fizycznych oraz pomiędzy tymi systemami" (Ibidem, s. 8). Warto również przytoczyć opracowaną na gruncie filozofii definicję Arkadija D. Ursuła, który uznał ją za odbicie różnorodności cechującej otaczającą rzeczywistość. Co za tym idzie, może to być zjawisko, proces, obiekt lub zdarzenie (Ibidem, s. 8). Mając na uwadze tę różnorodność, termin *rewolucji informacyjnej* podkreśla zasadnicze znaczenie nie tylko rozwoju technologii informacyjnych i komunikacyjnych (ICT), ale także fundamentalną rolę odgrywaną przez samą informację. Przede wszystkim akcentuje się tu łatwiejszy do niej dostęp oraz nowe możliwości jej przetwarzania i archiwizowania. Przy czym, jak trafnie zauważyła Agnieszka Jeran (2003: 213—214), zgodnie z zasadami cybernetyki „samo podkreślenie znaczenia informacji (jej przetwarzania) niczego do analizy nie wnosi, każdy bowiem otwarty system, a więc wszystko, co żyje, przetwarza informację". W związku z tym zaproponowała ona takie rozumienie przetwarzania informacji, które można zdefiniować jako wymianę, korzystanie z istniejących zasobów i opieranie na nich aktywności społecznej (Ibidem, s. 213—214). Rezultatem omówionych wyżej procesów stało się więc silne zaakcentowanie wiedzy, np. w gospodarce.

Tymczasem drugie często stosowane pojęcie *rewolucji (tele)informatycznej* jest terminem nieco węższym, zwracającym uwagę przede wszystkim na najistotniejsze procesy w wymiarze naukowo-technicznym i ich społeczne konsekwencje. Warto tutaj odwołać się do definicji zaproponowanej przez Marka Madeja (2009: 20—21), który uznał, iż istotą rewolucji informatycznej było

> szybkie upowszechnienie się i umasowienie tego rodzaju technologii, powodujące głębokie przekształcenia w ramach niemal każdej sfery stosunków społecznych, i powstanie nowego modelu społeczeństwa (a przynajmniej uformowanie się jego dodatkowego elementu, bardzo istotnego i silnie zintegrowanego z pozostałymi).

Jego zdaniem zmiany te mają charakter wielopłaszczyznowy (w skali lokalnej, państwowej, międzynarodowej, globalnej) i wieloaspektowy (ekonomia, wojskowość, nauka, polityka, sposoby spędzania czasu, więzi społeczne). W takim ujęciu oczywiście kategoria *informacji* również ma zasadnicze znaczenie, nie jest ona jednak kluczowym punktem odniesienia prowadzonych rozważań.

Jakkolwiek termin *rewolucja informacyjna* należy uznać za szerszy, wydaje się, iż jest on mniej przydatny do analizy zagadnień związanych z funkcjonowaniem państw w cyberprzestrzeni. W tym wypadku szczególne znaczenie mają bowiem kwestie związane właśnie z procesem upowszechnienia technologii informatycznych (teleinformatycznych) oraz wynikających z tego konsekwencji na wielu płaszczyznach i w wielu ujęciach. Poniższa analiza, biorąc pod uwagę fundamentalną rolę kategorii, jaką stała się współcześnie *informacja*, skupi się jednak głównie na próbie wskazania najistotniejszych etapów, cech i reperkusji rewolucji informatycznej.

Charakteryzując to zagadnienie, należałoby rozpocząć od wieku XIX, obfitującego w szereg istotnych odkryć naukowych, które przyczyniły się do zapoczątkowania szybkiego postępu technologicznego. Przede wszystkim na przełomie lat 30. i 40. pojawił się pierwszy telegraf elektryczny, który spowodował zasadnicze zmiany w dotychczasowej komunikacji między ludźmi. O jego znaczeniu świadczy fakt, iż współcześnie sieć telegraficzną określa się często mianem „wiktoriańskiego Internetu", który zrewolucjonizował wymianę informacji na duże odległości. Dwa kolejne istotne wydarzenia nastąpiły w drugiej połowie XIX wieku. W 1876 roku Aleksander Graham Bell wynalazł telefon, a w 1893 roku Nikola Tesla po raz pierwszy dokonał publicznej transmisji sygnału radiowego. Oba te osiągnięcia w następnych dekadach umożliwiły nie tylko postęp w zakresie komunikacji, ale także dały podstawę rozwoju pierwszych sieci komputerowych w ponad pół wieku później[2]. Równolegle toczyła się na świecie dyskusja na temat stworzenia automatycznej maszyny liczącej[3]. Na tym tle warto

[2] A. Onifade: *History of the Computer*. University of Ibadan: www.ieeeghn.org/wiki/images/5/57/Onifade.pdf; dostęp: 26.06.2013; A. Tatnall: *History of Computer Hardware and Software Development*. Encyclopedia of Life Support Systems: www.eolss.net/Sample-Chapters/C15/E6-45-12.pdf; dostęp: 26.06.2013; S. Deffree: *Tesla gives 1st public demonstration of radio, March 1, 1893*. EDN Network, 01.03.2014: www.edn.com/electronics-blogs/nikola-tesla/4408090/Tesla-gives-1st-public-demonstration-of-radio--March-1--1893; dostęp: 7.08.2014.

[3] Warto mieć świadomość, iż samo słowo *komputer* pochodzi od łacińskiego słowa *computāre*, oznaczającego 'liczyć' lub 'sumować'. Termin ten pierwotnie oznaczał maszynę, któ-

przytoczyć słowa Piotra Gawrysiaka (2008: 79—80), który zauważył, iż pod koniec XIX wieku rozwój naukowo-techniczny był już na tyle zaawansowany, iż pomysły automatyzacji obliczeń matematycznych przestały być jedynie egzotyczną ideą. Technologia ta nie była jednak ani odpowiednio rozwinięta, ani na tyle popularna i tania, aby trafić do produkcji masowej.

Z czasem coraz bardziej rosła jednak potrzeba opracowania komputera, uniwersalnego urządzenia, które przyczyniłoby się do ułatwienia różnorodnych obliczeń, w tym np. spisu ludności. Był to czynnik, który przyczynił się do przyspieszenia prac nad nim na początku XX wieku. Ich rezultatem było stworzenie w 1937 roku przez Bell Telephone Labs pierwszej binarnej maszyny sumującej o nazwie Model K. W tym samym roku John Vincent Atanasoff rozpoczął prace nad pierwszym komputerem elektronicznym. Jego dorobek został później wykorzystany do budowy maszyny ENIAC. W 1938 roku Konrad Zuse stworzył natomiast binarną maszynę liczącą V1, a na jej podstawie opracował w 1941 roku pierwszy programowalny kalkulator — V3. Warto zauważyć, iż maszyny te znalazły zastosowanie przemysłowe. W rozwiniętej wersji V4 komputer Zusego aż do połowy lat 50. XX wieku stanowił jedyny działający komputer w Europie. W 1942 roku John Atanasoff oraz Clifford Berry zbudowali elektroniczną maszynę liczącą ABC (Atanasoff-Berry Computer)[4]. W 1940 roku powstał również Bell Complex Number Calculator (CNC). W tym czasie opracowano także Harvard Mark I, znany także jako IBM Automatic Sequence Controlled Calculator oraz brytyjski Colossus, który był wykorzystywany w trakcie wojny do łamania niemieckich szyfrów. Bardzo ważnym wydarzeniem był moment zbudowania maszyny ENIAC — Electrical Numerical Integrator And Computer. Prace nad nią rozpoczęły się podczas drugiej wojny światowej, projekt stworzyli John Presper Eckert oraz John Mauchly. Pierwotnym zastosowaniem tej maszyny miały być obliczenia balistyczne dla potrzeb armii Stanów Zjednoczonych. Budowa została zakończona ostatecznie 14 lutego 1946 roku na Uniwersy-

---

rej głównym zadaniem było liczenie. Co ciekawe, pierwszy poważny krok w kierunku zbudowania maszyny liczącej postawiono już w 1694 roku. Wówczas mechaniczny kalkulator skonstruował wielki niemiecki filozof i matematyk Gottfried Wilhelm Leibniz, motywując swoje działania stwierdzeniem, iż „nie godzi się wybitnym ludziom trwonić czas na niewolniczą pracę, na obliczenia, które z zastosowaniem maszyn mógłby robić ktokolwiek". Innym istotnym osiągnięciem w tej dziedzinie było zaprojektowanie przez Charlesa Babbage'a w 1833 roku pierwszej maszyny analitycznej, której zasady działania miały być zbliżone do współczesnych komputerów cyfrowych. Zob. A. Adamski, 2012: 30; Gawrysiak, 2008: 34—68; Goban-Klas, Sienkiewicz, 1999: 20; Geers, 2011: 19; Fulmański, Sobieski, 2004: 17—22; *Compute*, The Free Dictionary: www.thefreedictionary.com/compute; dostęp: 22.06.2013.

[4] B. Carlson, A. Burgess, C. Miller: *Timeline of Computing History*. IEEE Computer Society: www.computer.org/cms/Computer.org/Publications/timeline.pdf; dostęp: 22.06.2013; D. Mukhopadhyay: *A Brief History of Computing*: http://cse.iitkgp.ac.in/~debdeep/teaching/CS130/slides/computers.pdf; dostęp: 22.06.2013; *History of Computers*: www.csi.ucd.ie/staff/jcarthy/home/CourseNotes/History%20%20+%20chips.pdf; dostęp: 22.06.2013.

tecie Pensylwańskim. Mimo ogromnych gabarytów moc obliczeniowa ENIAC-a była porównywalna ze współczesnymi kalkulatorami. Wykorzystywano go aż do 1955 roku[5].

Warto zauważyć, iż nie ma pełnej zgody ekspertów co do tego, która z wymienionych maszyn była pierwszym komputerem w historii. Według części badaczy na miano to zasługują maszyny skonstruowane m.in. przez Konrada Zusego, Johna Atanasoffa czy brytyjski Colossus. Według innych cechy pełnoprawnego komputera nosił dopiero ENIAC, co jednak rodzi dziś spore wątpliwości. W tym kontekście za pierwszy w pełni programowalny komputer elektroniczny uznaje się najczęściej powstały w 1943 roku Colossus. Jak bowiem zauważył Piotr Gawrysiak, z czysto technicznego punktu widzenia sława ENIAC-a była zdecydowanie niezasłużona, odznaczał się on bowiem dość prostymi i przestarzałymi rozwiązaniami. Z drugiej jednak strony ENIAC doprowadził do pojawienia się wykwalifikowanej kadry na rynku pracy (Gawrysiak, 2008: 133). Warto również zauważyć, iż zdaniem Daniela S. Pappa, Davida S. Albertsa oraz Alissy Tuyahov (1997: 14) to właśnie w tym czasie zakończyła się „pierwsza współczesna rewolucja informacyjna", za której początek autorzy uznali pojawienie się istotnych wynalazków telekomunikacyjnych w połowie XIX wieku.

Nie ulega wątpliwości, iż to w latach 40. XX wieku należy upatrywać początków długotrwałego procesu digitalizacji, którą można rozumieć w ujęciu technicznym jako „proces przetwarzania elektrycznego sygnału analogowego (ciągłego w funkcji czasu) na dyskretny ciąg cyfr, najczęściej binarnych, reprezentowanych w torze przesyłowym przez impulsy elektryczne o unormowanym kształcie" (Adamski, 2012: 40—41). Według Grahama Murdocka i Petera Goldinga oznaczała ona natomiast

> przekształcenie różnorodnych sposobów komunikacji […] w uniwersalną formę elektronicznych ciągów binarnych, pozwalających na szybkie przekształcenie danej formy w dowolną inną oraz na przechowywanie, odtwarzanie, manipulowanie i dystrybuowanie każdej z nich z bezprecedensową łatwością[6].

---

[5] K. Geers, 2011: 19; *Electrical Numerical Integrator and Computer*. United States Patent Office, 04.02.1964; J. Duba: *Historia komputerów osobistych*: www.jakubduba.pl; dostęp: 22.06.2013; K. Kempf: *Electronic Computers within the Ordonance Corps*: http://ftp.arl.mil/~mike/comphist/61ordnance/chap2.html; dostęp: 22.06.2013; B. Carlson, A. Burgess, C. Miller: *Timeline of Computing History*. IEEE Computer Society: www.computer.org/cms/Computer.org/Publications/timeline.pdf; dostęp: 22.06.2013; D. Mukhopadhyay: *A Brief History of Computing*: http://cse.iitkgp.ac.in/~debdeep/teaching/CS130/slides/computers.pdf; dostęp: 22.06.2013; *History of Computers*: www.csi.ucd.ie/staff/jcarthy/home/CourseNotes/History%20%20+%20chips.pdf; dostęp: 22.06.2013.

[6] W tej perspektywie kod binarny obejmuje zapis w systemie zero-jedynkowym, a bit (*binary digit*) jest „najmniejszą ilością informacji, potrzebną do określenia, który z dwóch stanów (równie prawdopodobnych) przyjął układ". Na bajt natomiast składa się 8 bitów. Dane zapisane w formie binarnej mogą być odtworzone przez odpowiednie oprogramowanie, które może z nich odtworzyć np. obraz lub dźwięk (zob. Adamski, 2012: 40—41).

W tym kontekście warto zauważyć, iż komputery elektroniczne, które powstały w latach 40. XX wieku, odznaczały się jeszcze jedną cechą istotną z punktu widzenia postępu technologicznego. W odróżnieniu od wcześniejszych kalkulatorów mechanicznych wykorzystywały one fale elektromagnetyczne do manipulowania natężeniem prądu. Procesy zachodzące w komputerach miały, zdaniem Agnieszki Rothert (2004: 38—39), charakter niebezpośredni i niewidzialny dla ludzi, co komplikowało sposób postrzegania świata na zasadzie: natura / kultura, człowiek / technologia, istnienie / czas. Według autorki komputery i ich oprogramowanie stały się więc na pozór „materią nieożywioną wykorzystywaną przez człowieka jako narzędzia", otwierając jednakże przed nim „inne przestrzenie czy też hiperrzeczywistości".

Omówione wyżej osiągnięcia technologiczne stanowiły zaledwie sygnał do podjęcia bardziej zaawansowanych prac w tej dziedzinie w kolejnych latach. Jednym z pierwszych istotnych ich rezultatów było opracowanie pierwszego tranzystora w 1947 roku przez Bell Telephone Labs. O jego znaczeniu świadczył fakt, iż jego projektanci w 1956 roku zostali uhonorowani nagrodą Nobla. W 1951 roku twórcy ENIAC-a zbudowali natomiast kolejny komputer — UNIVAC. Od swojego poprzednika odróżniał się nie tylko nowymi rozwiązaniami konstrukcyjnymi, lecz także odmiennym zastosowaniem. Jako pierwszy w historii został on wykorzystany w celach komercyjnych, jego moc obliczeniowa ułatwiła i przyspieszyła bowiem spis ludności w Stanach Zjednoczonych. Miarą jego sukcesu był fakt, że sprzedano aż 46 maszyn tego typu, każdą za cenę ok. 1 miliona dolarów. Powodzenie UNIVAC-a pociągnęło za sobą kolejne istotne osiągnięcia w tej dziedzinie. Szczególną rolę odegrała tu firma IBM, która w 1953 roku stworzyła urządzenie o nazwie 650. Był to pierwszy komputer wyprodukowany w większej liczbie egzemplarzy — ok. 1,5 tysiąca sztuk. Jego następcą szybko stał się IBM 701. W tym samym czasie powstała również pierwsza drukarka (Uniprinter) oraz komputer oparty na tranzystorach (w 1955 roku). W 1956 roku powstał także pierwszy twardy dysk, stworzony przez IBM (RAMAC). Istotnych odkryć dokonano ponadto w 1958 roku, kiedy Bell Telephone opracowało pierwszy modem umożliwiający transfer danych w formie binarnej. W tym samym roku firma Texas Instruments przygotowała również prototyp układu scalonego, będącego później podstawową technologią produkcji komputerów[7].

Wszystkie wymienione wyżej osiągnięcia z lat 30., 40. i 50. XX wieku dały solidną podstawę idei stworzenia zintegrowanej sieci komputerów umożliwiającej wielostronny transfer danych (Goban-Klas, Sienkiewicz, 1999: 25—26). Źródeł tej idei, jak zauważył Marek Pudełko, należy upatrywać w zapoczątkowaniu

[7] Haigh, 2004: 5—26; B. Carlson, A. Burgess, C. Miller: *Timeline of Computing History*. IEEE Computer Society: www.computer.org/cms/Computer.org/Publications/timeline.pdf; dostęp: 22.06.2013; D. Mukhopadhyay: *A Brief History of Computing*..., op.cit.

wyścigu kosmicznego między Stanami Zjednoczonymi a Związkiem Radzieckim w drugiej połowie lat 50. XX wieku. Gdy ZSRR wystrzelił pierwszego satelitę Sputnik, władze USA doszły do wniosku, iż nie są w stanie zapobiec ewentualnemu uderzeniu zbrojnemu z przestrzeni kosmicznej. Doprowadziło to w Stanach Zjednoczonych do intensyfikacji wysiłku naukowo-technicznego skierowanego na rozwój nowych technologii, zarówno kosmicznych, jak i komputerowych. W tym celu w 1958 roku powołano Agencję Zaawansowanych Projektów Badawczych (Advanced Research Projects Agency — ARPA), która miała koordynować wysiłki na styku sił zbrojnych i środowiska naukowego oraz odzyskać dla USA palmę pierwszeństwa w tej dziedzinie. To właśnie w tej sytuacji, w ramach ARPA pojawiła się po raz pierwszy idea stworzenia sieci komputerowej. W literaturze przedmiotu wskazuje się z reguły na dwa rodzaje bezpośrednich motywacji, które stały za tymi pomysłami. Część specjalistów wspomina o potrzebie *stricte* wojskowej. Według nich, obawiając się konsekwencji ewentualnego ataku atomowego ze strony Związku Radzieckiego, władze amerykańskie pragnęły stworzyć obejmującą cały kraj sieć połączonych ze sobą komputerów, dzięki której paraliż systemu obronnego byłby niemożliwy. W rzeczywistości jest to jednak mit. Prawdziwym powodem pojawienia się idei sieci połączonych ze sobą komputerów była natomiast potrzeba samych naukowców pracujących dla agencji. Jak zauważył jeden z ojców Internetu, Leonard Kleinrock, dzięki umożliwieniu wielostronnej komunikacji między komputerami eksperci z ARPA pragnęli ułatwić sobie proces wymiany danych, w tym m.in. oprogramowania bądź wyników badań, pomysł stworzenia sieci komputerowej miał zatem pierwotnie charakter wyłącznie cywilny (Pudełko, 2013: 17—18; Cohen-Almagor, 2011: 46—47). Ideom tym sprzyjał postępujący proces rozwoju technologii komputerowych na przełomie lat 50. i 60. XX wieku. Jednym z istotniejszych jego przejawów było opracowanie przez Texas Instruments w 1961 roku pierwszego komputera opartego na układach scalonych i pamięci półprzewodnikowej.

Charakteryzując genezę powstania Internetu, nie można również pominąć pomysłu Josepha Carla Licklidera. W latach 1962—1963 wysunął on koncepcję ICN (Intergalactic Computer Network). Według opracowanego przez niego memorandum głównym problemem, który stał na przeszkodzie realizacji tej koncepcji, było opracowanie jednolitego standardu komunikacji. Sam pomysł przypominał natomiast współczesną formę Internetu, polegał bowiem na stworzeniu globalnej sieci wzajemnie połączonych komputerów umożliwiających szybki dostęp do danych oraz specjalistycznego oprogramowania. Licklider wraz z prowadzoną przez siebie grupą badaczy rozpoczął w październiku 1962 roku prace nad tym projektem w ramach ARPA. Pierwsze terminale sieciowe wykorzystywane do badań zainstalowano w Santa Monica, na Uniwersytecie Kalifornijskim w Berkeley oraz w Massachusetts Institute of Technology (MIT). Wskazane przez Licklidera problemy techniczne zostały w dużej mierze prze-

zwyciężone dzięki metodzie „przełączania pakietów" opracowanej przez Paula Barana, Donalda Daviesa oraz wspomnianego już Leonarda Kleinrocka. Pomysły sformułowane przez tę grupę zyskały zainteresowanie szefa ARPA Roberta Taylora, który zlecił Larry'emu Robertsowi z MIT fizyczne stworzenie sieci nazwanej ARPANET (Lakomy, 2013: 26—40; Pudełko, 2013: 20—23; Cohen-Almagor, 2011: 47—48). Warto przy tym zauważyć, iż wysiłki te wpisały się w dynamiczny postęp telekomunikacji na innych polach: przykładowo w 1964 roku wystrzelono na orbitę pierwszego cywilnego satelitę telekomunikacyjnego Syncom III. Był to początek szybkiego rozwoju komercyjnej komunikacji satelitarnej (Papp, Alberts, Tuyahov, 1997: 27).

Pierwsze dwustronne połączenie w sieci ARPANET miało miejsce 29 października 1969 roku o godzinie 22.30 między komputerami znajdującymi się na Uniwersytecie Kalifornijskim oraz w Stanford Research Institute. W ciągu miesiąca do ARPANET-u podłączono kolejne dwa komputery, tym razem w Utah oraz w Santa Barbara, a ich wzajemną komunikację oparto na protokole NCP (Network Control Protocol)[8]. Nie ulega wątpliwości, iż wydarzenie to miało rewolucyjne znaczenie i stanowiło pierwszy krok na drodze do ustanowienia globalnej sieci z wizji Josepha Carla Licklidera. W kolejnych latach pierwsza sieć komputerowa zaczęła się szybko rozrastać. W czerwcu 1970 roku istniało już 9 węzłów sieci, w grudniu 1970 roku — 13, a na początku 1972 roku aż 23. W połowie lat 70. ARPANET obejmowała 57 wzajemnie połączonych ośrodków. Co ciekawe, do sieci podłączono także pierwsze komputery znajdujące się poza USA, przede wszystkim z Wielkiej Brytanii oraz Norwegii. W rezultacie na początku lat 80. na ARPANET składało się aż 213 węzłów, co świadczyło o jego rosnącym potencjale międzynarodowym[9]. W tym kontekście należałoby zwrócić uwagę na kilka doniosłych cech tej pierwszej sieci komputerowej. Przede wszystkim miała ona wówczas charakter elitarny, dostęp do niej miało bowiem jedynie wąskie grono naukowców. Po drugie warto przywołać słowa Andrzeja Adamskiego (2012: 33), który scharakteryzował jej najważniejsze właściwości techniczne. Jego zdaniem:

> u podstaw idei Internetu leży zasada decentralizacji (równorzędności wszystkich węzłów) oraz redundancji funkcji sieci — dzielenia przesyłanych danych na drobne fragmenty (pakiety), które są przekazywane są najszybszą możliwą trasą do odbiorcy i tam na powrót scalane. Decentralizacja zakłada, że system

[8] Protokół komunikacyjny opisuje szczegółowo sposób postępowania w danym aspekcie komunikacji między komputerami, uwzględnia np. działania podejmowane w wypadku wystąpienia błędów, może definiować niskopoziomowe parametry łącza (np. poziomy napięć czy rodzaj sygnału) lub mechanizmy warstw wyższych (takie jak format komunikatów). Za: Comer, 2012: 36.

[9] Zob. Pudełko, 2013: 23—40; M. Horvath: *The Evolution of the Information Revolution. The Growing Power of Virtual Social Networks*: http://library.uniteddiversity.coop/Systems_and_Networks/The_Evolution_of_the_Information_Revolution.pdf; dostęp: 25.07.2013.

> nie ma komunikacyjnego centrum, przez które miałyby przepływać wszystkie informacje i które kieruje działaniem wszystkich pozostałych części. Kolejną zasadą jest rozproszona moc obliczeniowa, tak aby elementy systemu mogły ze sobą współpracować, a poszczególne składniki systemu — sumować się.

Taka architektura była o tyle istotna, iż nawet w sytuacji częściowej awarii sieci komunikacja mogła ominąć niefunkcjonujące fragmenty (Ibidem, s. 33). Po trzecie: ciekawą opinię sformułował Ron Deibert (2013: 4—8), według którego podstawową zasadą, na której tworzony był pierwotny Internet, było zaufanie do jego użytkowników. To właśnie ta cecha w zasadniczym stopniu wpłynęła na ukształtowanie się jego otwartej architektury, która w późniejszym czasie okazała się pewnym problemem ze względu na wymogi bezpieczeństwa.

Ważnym momentem w rozwoju ARPANET-u był początek lat 70., kiedy zaczęto opracowywać wykorzystywany do dziś w Internecie protokół TCP/IP (Transmission Control Protocol/Internet Protocol). Do użytku wojskowego został oddany już w 1980 roku. Sam ARPANET zaczął stosować te nowe rozwiązania dopiero w 1983 roku, kiedy zrezygnowano z przestarzałego protokołu NCP. Co ciekawe, to właśnie w tym kontekście po raz pierwszy w historii wykorzystano termin *Internet*. Pojawił się on w artykule ojców ARPANET-u Vintona Cerfa i Roberta Khana z 1973 roku, poświęconym rezultatom prac zespołu Network Working Group (Castells, 2003: 21). Bez wątpienia opracowanie protokołu TCP/IP przyczyniło się w zasadniczym stopniu do stworzenia globalnej sieci, stanowił bowiem jednolity i efektywny standard wymiany informacji (Cohen-Almagor, 2011: 50—51). Istotne znaczenie miało również opracowanie w 1971 roku usługi FTP (File Transfer Protocol) umożliwiającej wymianę plików. Na początku lat 70. XX wieku doszło także do znacznego poszerzenia możliwości poczty elektronicznej. W 1971 roku jej dojrzałą formę opracował Ray Tomlinson, pracujący wówczas w firmie BBN Technologies. O znaczeniu tego odkrycia świadczył fakt, iż już w dwa lata później 75% całego ruchu w sieci ARPANET generowały e-maile. Warto również wspomnieć o wprowadzeniu usługi Telnet, która polegała na możliwości wykorzystania odległego, podłączonego do sieci serwera na tej samej zasadzie co własnego komputera. Za ojca tego rozwiązania uznaje się Stephena Carra, który podstawy tej usługi zaprezentował 25 września 1969 roku (Cohen-Almagor, 2011: 49—57; Kambil, 1997: 97).

Wszystkie omówione wyżej osiągnięcia przyczyniły się do znacznego przyspieszenia na obszarze teleinformatyki na przełomie lat 70. i 80. XX wieku. Zaczęły powstawać inne sieci komputerowe oparte na doświadczeniach i rozwiązaniach ARPANET-u, pomysł ten zatem powoli ewoluował w swoistą „galaktykę sieci" (Rothert, 2004: 41). Już w lipcu 1970 roku na Hawajach powstał ALOHANet. Była to pierwsza w historii sieć radiowa łącząca 5 węzłów na odległości przeszło 400 km. Stosunkowo szybko ALOHANet została połączona z ARPANET-em, co było możliwe dzięki wykorzystaniu łączy satelitarnych. Co

ważne, to na podstawie doświadczeń zdobytych na Hawajach udało się stworzyć zręby technologii Wi-Fi (Pudełko, 2013: 37—39). Nieco inne cechy posiadała stworzona w Wielkiej Brytanii sieć X.25. Miała ona odmienną od ARPANET-u architekturę, kładącą większy nacisk na wymogi bezpieczeństwa. Co ciekawe, funkcjonuje ona współcześnie, choć ze względu na małą przepustowość charakteryzuje się niewielką popularnością wśród użytkowników. Warto dodać, iż jako pierwszą w Europie połączono ją częściowo z ARPANET-em już w 1973 roku. Należy również wspomnieć o sieci NORSAR (Norwegian Seismic Array). Jej głównym celem było zbieranie informacji na temat aktywności sejsmicznej na świecie, co miało również zastosowanie wojskowe, związane z wykrywaniem próbnych wybuchów jądrowych. W 1973 roku NORSAR został podłączony do ARPANET-u dzięki transmisji satelitarnej (Ibidem, s. 39—43). Z kolei JANET (Joint Academic Network) powstała w Wielkiej Brytanii jeszcze w latach 70. XX wieku w celach naukowych i edukacyjnych[10].

Proces powstawania kolejnych sieci komputerowych przyspieszył jeszcze bardziej na początku lat 80. W 1981 roku stworzono BITNET (Because It's The Network), który bazował na serwerach IBM. Była to sieć o odmiennej od ARPANET-u architekturze. Przede wszystkim charakteryzowała się znacznym scentralizowaniem oraz wysokimi standardami bezpieczeństwa, rygorystyczną etykietą, brakiem anonimowości użytkowników oraz pełnym zakazem działalności politycznej i handlowej. Cieszyła się bogatymi jak na tamte czasy możliwościami związanymi z pocztą elektroniczną. Warto zauważyć, iż BITNET zyskał pewną popularność w Europie, gdzie na jego podstawie w 1985 roku powstała EARN (European Academic Research Network) łącząca najważniejsze ośrodki akademickie. W rywalizacji z ARPANET-em BITNET poniósł jednak porażkę, na co wpłynęły przede wszystkim jego poważne ograniczenia techniczne, spowodowane zarówno wykorzystywanymi urządzeniami IBM, jak i brakiem możliwości zaimplementowania protokołu TCP/IP[11].

W tym czasie równolegle powstawały inne, bardziej wyspecjalizowane sieci. Należy do nich zaliczyć m.in. MFENET, HEPNET, SPAN czy CSNET. MFENET oraz HEPNET zostały utworzone przez amerykański Departament Energii. Jako pierwsza, jeszcze w 1976 roku powstała MFENET, która umożliwiła wymianę danych między ośrodkami zajmującymi się badaniami nad energią termojądrową (MFE — Magnetic Fusion Energy). HEPNET rozpoczęła działal-

[10] J. Reid: *The Good Old Days: Networking in UK Academia ~ 25 Years Ago*. Manchester 2007: www.uknof.com/uknof7/Reid-History.pdf; dostęp: 23.06.2013.

[11] R. Watt: *A National Network (At Last...)*. In: *A Nation Goes Online*. Ed. G. Miller. Institute CA.NET: http://its.dal.ca/publications/history/CAnet/index.html; dostęp: 23.06.2013; A. Thompson: *The History of the Internet in Nova Scotia*, s. 12—13: http://its.dal.ca/publications/history/NSbuilding/history.pdf; dostęp: 23.06.2013. *BITNET on MTS*. Information Technology Divison, University of Michigan 1990: http://bitsavers.informatik.uni-stuttgart.de/pdf/univOfMichigan/mts/memos/r1039-BitnetOnMTS-Sep1990.pdf; dostęp: 23.06.2013.

ność cztery lata później w celu wymiany informacji dotyczących fizyki wysokich energii (HEP — High Energy Physics). W połowie lat 80. XX wieku obie zostały połączone przez Departament Energii w ESnet (Energy Sciences Network), która funkcjonuje do dziś[12]. SPAN (Space Physics Analysis Network) została stworzona przez amerykańską agencję NASA na początku lat 80. XX wieku i szybko stała się platformą współpracy i wymiany opinii naukowców zajmujących się szeroko pojętymi badaniami kosmosu. O jej dynamicznym rozwoju świadczył fakt, iż w 1988 roku w jej ramach działało już ok. 2000 komputerów, w głównej mierze zlokalizowanych w największych ośrodkach badawczych w USA i na świecie. Warto dodać, iż SPAN była połączona z kilkoma innymi sieciami, w tym m.in. z HEPNET, BITNET, JANET oraz ARPANET (Green, 1988: 205—213). CSNET (Computer Science Network) była natomiast kolejną siecią naukową, która powstała w Stanach Zjednoczonych w 1981 roku. Została ona utworzona przez U.S. National Science Foundation w celu wymiany informacji między badaczami, którzy nie mieli wówczas dostępu do ARPANET-u. Głównym zamysłem twórców CSNET było więc stworzenie jej odpowiednika, który byłby dostępny dla szerszego grona naukowców z całego świata. Dzięki tym założeniom oraz wsparciu agencji DARPA CSNET szybko się rozwinęła, w 1984 roku obejmując aż 84 węzły. W końcowym okresie funkcjonowania na CSNET składała się ok. 180 ośrodków. CSNET odegrała istotną rolę w popularyzacji idei Internetu w tych środowiskach, które nie mogły w latach 80. XX wieku skorzystać z ARPANET-u. W 1988 roku CSNET połączyła się z BITNET, tworząc nową sieć zorganizowaną przez Corporation for Research and Educational Networking[13]. Warto również wspomnieć o pomyśle sieci USENET, który pojawił się w 1979 roku. Rok później został on wdrożony przez Toma Truscotta i Jima Ellisa. Był to *de facto* prekursor współczesnych forów dyskusyjnych. Wówczas była to pierwsza usługa sieciowa, która udostępniła użytkownikom miejsce i narzędzia swobodnej i wielostronnej wymiany poglądów (Bógdał-Brzezińska, Gawrycki, 2003: 48—50; Lakomy, 2013: 37—39).

W tym kontekście warto jeszcze wspomnieć o pojawieniu się na początku lat 80. XX wieku unikalnej sieci FIDONET, która powstała dzięki wprowadzeniu na rynek modemu Smartmodem. Pozwolił on na stworzenie systemów BBS (Bulletin Board System), będących pewnego rodzaju elektronicznymi tablicami ogłoszeniowymi. Była to jednak usługa o charakterze lokalnym, co utrudniało wykorzystanie jej w skali kraju lub świata. Przełomowym momentem w rozwoju BBS-ów było opracowanie w 1984 roku oprogramowania, które automatycznie wymieniało dane pomiędzy różnymi systemami BBS, co w efekcie doprowadziło do powstania FIDONET. W odróżnieniu od architektury właściwej dla

[12] Zob. Martin, 2012; Energy Sciences Network, U.S. Department of Energy: http://science.energy.gov/ascr/facilities/esnet; dostęp: 23.06.2013; Sampson, Hair, eds., 1990: 274.

[13] *CSNet — Computer Sciences Network*. Living Internet: www.livinginternet.com/i/ii_csnet.htm; dostęp: 23.06.2013.

ARPANET-u sieć ta nie składała się z połączonych na stałe elementów. Wynikało to przede wszystkim z oparcia jej o stosunkowo drogie połączenia telefoniczne, przez co wymiana danych musiała być krótkotrwała i skondensowana. Warto zauważyć, iż ten rodzaj komunikacji elektronicznej bardzo szybko zyskał dużą popularność. Świadczył o tym fakt, iż jeszcze w połowie lat 90. XX wieku w skład FIDONET-u wchodziło aż 30 000 systemów BBS, choć później popularność tego typu rozwiązań znacząco spadła (Gawrysiak, 2008: 239—240).

Z drugiej strony od początku lat 70. XX wieku doszło do dalszego przyspieszenia postępu w dziedzinie technologii komputerowych. Już w latach 1970 i 1971 zaprezentowano całą gamę przełomowych osiągnięć: pierwsze na świecie dynamiczne pamięci RAM firmy Intel, mikroprocesory oraz dyskietki (*floppy disk*). Po raz pierwszy na większą skalę skupiono się również na ułatwieniu komunikacji człowieka z komputerem, czego przejawem były nowe interfejsy graficzne (GUI — Graphical User Interface) (Adamski, 2012: 31). Dzięki temu technologie te, dostępne dotychczas wyłącznie dla wąskiego grona specjalistów, zaczęto upowszechniać oraz wykorzystywać do celów komercyjnych. Symbolem tych tendencji było opracowanie w 1973 roku Xerox Alto, jednego z pierwszych eksperymentalnych komputerów osobistych. Co prawda został on sprzedany zaledwie w 2000 egzemplarzy, wyznaczył jednak pewien standard dla kolejnych generacji tego typu urządzeń. Posiadał nie tylko monitor, ale także zewnętrzne dyski twarde i procesory wykonane w technologii układów scalonych oraz kartę sieciową, która umożliwiała podłączenie go do lokalnej sieci Ethernet. Co więcej, Alto posiadał bardzo zaawansowane jak na tamte czasy oprogramowanie, w tym edytory tekstu i grafiki (Gawrysiak, 2008: 191—193). Do upowszechnienia się tego typu technologii w znacznym stopniu przyczynił się również komputer Altair 8800, który charakteryzował się przede wszystkim niewielką ceną. Zaprojektowany przez MITS w 1974 roku, był skierowany głównie do entuzjastów elektroniki, osiągając jednak stosunkowo dużą popularność. Zdaniem Piotra Gawrysiaka (2008: 211—218) to od niego zaczęła się rewolucja informatyczna, polegająca na lawinowym wzroście zainteresowania informatyką. W tym czasie popularne stały się również kieszonkowe kalkulatory oraz pierwsze bardziej skomplikowane gry komputerowe, które stały się kolejnym impulsem rozwijającym społeczne zainteresowanie nowymi technologiami. Równolegle zmianom tym towarzyszył proces powstawania nowych języków programowania oraz urządzeń i aplikacji ułatwiających codzienne wykorzystanie komputerów. W połowie lat 70. pojawiły się np. pierwsze drukarki laserowe i atramentowe oraz systemy operacyjne. W 1976 roku powstał pierwszy komputer stworzony przez Apple (Apple 1). Prawdziwa rewolucja, tym razem komercyjna, nastąpiła jednak dopiero na początku lat 80. XX wieku. W 1981 roku firma IBM stworzyła pierwszy komputer osobisty PC (Personal Computer). Charakteryzował się on nie tylko elastyczną architekturą, ale także wysoką jakością wykonania, zaawansowanymi rozwiązaniami sprzętowymi oraz użytecznym

oprogramowaniem. Powstały wówczas również inne komputery domowe, tworzone między innymi przez Commodore oraz Atari. W połowie lat 80. firma Microsoft stworzyła natomiast pierwszy program Windows, który w latach 90. przekształcił się w popularny system operacyjny[14].

Na tym tle widać więc wyraźnie, iż w ciągu zaledwie dwóch dekad dokonała się rewolucyjna zmiana, jeśli chodzi o zastosowanie technologii komputerowych. Charakteryzowała się ona przede wszystkim utratą przez nie elitarnego charakteru. Komputery stopniowo zaczęły się stawać urządzeniami pożądanymi w każdym domu. Co więcej, ich ówczesne osiągnięcia wielokrotnie już przewyższały moc obliczeniową pierwszych, niezwykle drogich komputerów, takich jak ENIAC i UNIVAC. Warto przy tym zauważyć, iż doszło do rozejścia się prac w tej dziedzinie w dwóch kierunkach. Jeden miał charakter głównie komercyjny i wynikał z rosnącego popytu na codzienne zastosowanie nowych urządzeń do celów rozrywkowych bądź biznesowych, drugi kierunek miał natomiast charakter bardziej profesjonalny i skupiał się na tworzeniu wyspecjalizowanych superkomputerów, które byłyby przydatne wyłącznie do badań naukowych lub celów militarnych.

Częściowe upowszechnienie komputerów osobistych oraz coraz szersze możliwości ich pozanaukowego i pozawojskowego wykorzystania stanowiły impuls, który przyczynił się do dalszego rozwoju sieci. Świadczyły o tym przemiany, które następowały od początku lat 80. XX wieku. Projekt ARPANET, bez względu na jego znaczenie dla środowiska naukowego, nie do końca współgrał z zadaniami, które miała realizować agencja ARPA (przekształcona w marcu 1972 roku w Defense Advanced Research Projects Agency — DARPA). W związku z tym pojawiły się głosy, które sugerowały wykorzystanie tych doświadczeń i osiągnięć do celów *stricte* wojskowych. W konsekwencji w 1983 roku, wraz z wprowadzeniem nowego standardu protokołu TCP/IP, powołano odrębną sieć wojskową Stanów Zjednoczonych MILNET (Military Network). Obie sieci — ARPANET wykorzystywany w celach komunikacyjnych oraz wojskowy MILNET — zostały od siebie ostatecznie odseparowane ze względów bezpieczeństwa[15] i od tej pory obie rozwijały się samodzielnie. W latach 80. XX wieku sieć wojskowa określana była mianem DDN (Defense Data Network) i była obsługiwana przez amerykański Departament Obrony. Objęła ona swoim działaniem nie tylko system obronny Stanów Zjednoczonych, ale także bazy zagraniczne. Została podzielona na cztery podsieci: MILNET dla jawnych danych, DSNET 1

[14] Wcześniej był nakładką na system operacyjny MS-DOS. Zob. B. Carlson, A. Burgess, C. Miller: *Timeline of Computing History*. IEEE Computer Society: www.computer.org/cms/Computer.org/Publications/timeline.pdf; dostęp: 22.06.2013; D. Mukhopadhyay: *A Brief History of Computing*, op.cit. Szerzej na ten temat piszą Fulmański, Sobieski, 2004: 22—27.

[15] Należy podkreślić, iż separacja nie była pełna. Nie było początkowo takiego wymogu, gdyż w sieci MILNET wykorzystywano tylko jawne dane. Zob. *What is MILNet*. Tech-FAQ: www.tech-faq.com/milnet.html; dostęp: 23.06.2013.

dla ruchu tajnego, DSNET 2 dla ruchu o poziomie tajności TOP SECRET oraz DSNET 3 dla danych o poziomie tajności TOP SECRET/SCI. Warto dodać, że sam DDN został w późniejszym czasie rozdzielony na trzy oddzielne sieci o odmiennej specyfikacji. Pierwszą z nich był NIPRNet (Non-Classified Internet Protocol Router Network), która zawierała dane jawne, mające jednak wysoką wrażliwość. SIPRNet (Secret Internet Protocol Router Network), która choć funkcjonowała w oparciu o tę samą architekturę, była zupełnie odrębną siecią; w odróżnieniu od NIPRNet zawierała dane poufne i tajne (aż do poziomu SECRET). Powstała także sieć JWICS (Joint Worldwide Intelligence Communications System), która obejmowała dane o poziomie tajności TOP SECRET i wyżej[16].

Moment rozdzielenia ARPANET-u oraz MILNET-u uznaje się za symboliczny początek funkcjonowania Internetu, składającego się z wielu połączonych ze sobą sieci komputerowych. Wydarzenie to w zasadniczym stopniu zdeterminowało dalsze prace naukowo-techniczne w tej dziedzinie. Jednym z istotniejszych ich kierunków było opracowanie w 1984 roku na Uniwersytecie Wisconsin usługi DNS (Domain Name System), która ułatwiła korzystanie z zasobów dostępnych w ARPANET. Rozumie się przez nią „system serwerów oraz protokół komunikacyjny zapewniający zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową"[17]. W uproszczeniu system ten odpowiada więc za odwzorowanie nazw symbolicznych, które są łatwiejsze do zapamiętania dla użytkowników, na adresy IP. DNS posiada strukturę hierarchiczną. Najistotniejszym segmentem nazwy (np. www.un.org) jest część ostatnia, zwana domeną najwyższego poziomu (TLD — Top-Level Domain). Część z TLD jest ogólnie dostępna, inne natomiast są przeznaczone dla określonych podmiotów, takich jak niepodległe państwa, organizacje niekomercyjne (.org), wojsko (.mil), instytucje rządowe (.gov), organizacje komercyjne (.com) czy instytucje edukacyjne (.edu)[18].

W tym czasie dynamicznie rozwijały się również same zasoby dostępne w ARPANET. Świadczył o tym fakt, iż w 1983 roku liczba jej serwerów (*host*) oscylowała w granicach 500. W połowie lat 80. XX wieku, jak twierdzili zgodnie „ojcowie Internetu", ARPANET była wyjątkową technologią, którą w coraz większym stopniu zaczęły wykorzystywać szersze grupy użytkowników, nie-

[16] C. Cornell: *A Brief History of MILNet*. Ezin Articles: http://ezinearticles.com/?A-Brief-History-of-MilNet&id=5726334; dostęp: 23.06.2013; Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff, 1997; *Secret Internet Protocol Router Network*. FAS.org: www.fas.org/irp/program/disseminate/siprnet.htm; dostęp: 23.06.2013; Pudełko, 2013: 73—74.

[17] *System DNS: czyli o tym, jak działa system zmiany nazw w Sieci*. Strefa Domeny, 12.08.2009. Za: Adamski, 2012: 36.

[18] Warto zaznaczyć, iż współcześnie zarządzaniem domenami najwyższego poziomu zajmuje się Internet Corporation for Assigned Names and Numbers (ICANN). Za: Comer, 2012: 98—99.

związanych bezpośrednio ze środowiskiem naukowym. Jednocześnie dalej ewoluowały inne sieci, przeznaczone wyłącznie dla badaczy i specjalistów. Oprócz ARPANET-u charakter taki miały wspomniana już brytyjska JANET oraz amerykańska NSFNET. Istotną rolę w procesie rozwoju Internetu odegrała właśnie ta druga. Została stworzona przez National Science Foundation w 1986 roku jako pierwsza amerykańska sieć szkieletowa. U podstaw jej funkcjonowania leżało pięć założeń:

1. Została oparta na powszechnym już standardzie protokołu TCP/IP.
2. Amerykańskie agencje rządowe miały uczestniczyć w kosztach rozwoju sieci, przede wszystkim jeśli chodzi o rozbudowę infrastruktury.
3. Miała być dostępna dla wszystkich ośrodków naukowych w USA.
4. NSF miało wspierać organizacje koordynujące rozwój sieci.
5. Miała być wykorzystywana wyłącznie do celów naukowych i edukacyjnych.

Szczególnie to ostatnie założenie rodziło pewne kontrowersje, gdyż istniało coraz większe zainteresowanie komercyjnym zastosowaniem możliwości rodzącego się Internetu. W konsekwencji sektor prywatny zaczął tworzyć własne sieci, które stopniowo zyskiwały dużą popularność. Dość szybko zaczęły się one ze sobą łączyć, co było zresztą stymulowane przez pierwszych komercyjnych dostawców usługi internetowej (Pudełko, 2013: 87—91; Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff, 1997: 104—105; Guisnel, 1997b: 218). Mając na uwadze te rozważania, warto odwołać się do słów Vintona Cerfa, który — jak się wydaje — najtrafniej oddał naturę rodzącego się wówczas Internetu: „ARPANET jest siecią komputerów. Internet jest siecią sieci”[19]. Manuel Castells (2003: 37—40) zauważył w tym kontekście, iż jego najistotniejszą cechą była wówczas otwartość architektury, zarówno w wymiarze technicznym, jak i społeczno-instytucjonalnym. Stało się to źródłem jego największej siły, czyli „samoewolucji”. Na tej podstawie ukuto ogólną definicję Internetu, według której jest to „sieć łącząca wiele innych sieci korzystających z protokołu TCP/IP […] połączonych za pośrednictwem bram i korzystających ze wspólnej przestrzeni adresowej” (Goban-Klas, Sienkiewicz, 1999: 26).

W drugiej połowie lat 80. XX wieku doszło jeszcze do kilku innych wydarzeń, które w zasadniczym stopniu wpłynęły na ukształtowanie współczesnego modelu Internetu, a szerzej: na oblicze początkowego stadium rewolucji informatycznej. W 1988 roku w sieci pojawił się złośliwy program komputerowy o nazwie *Internet Worm*. Został stworzony przez Roberta Morrisa Jr., który chciał w ten sposób uświadomić ówczesnym internautom potrzebę wprowadzenia odpowiednich zabezpieczeń. Udało mu się ten cel osiągnąć, był bowiem pierwszą i jak dotąd ostatnią osobą, która doprowadziła do niemal zupełnego

[19] Za: H. Haas: *Internet history. Why we are here?* 11.03.2005, s. 2: www.perihel.at/2/basics/37-Internet-History.pdf; dostęp: 24.06.2013.

paraliżu Internetu. Napisany przez niego program błyskawicznie rozprzestrzenił się po sieci, blokując działalność jej najistotniejszych elementów. Informatykom z największych światowych ośrodków naukowych dopiero po 8 dniach udało się opanować sytuację. Wydarzenie to stało się inspiracją do powołania pierwszego zespołu specjalistów, którego celem było przeciwdziałanie tego typu zagrożeniom — Computer Emergency Response Team (CERT) (Lakomy, 2013: 39—49; Pudełko, 2013: 90—91).

Drugim istotnym momentem było stworzenie systemu rozmów IRC (Internet Relay Chat), który ułatwił komunikację pomiędzy użytkownikami sieci. Do dynamicznego rozwoju Internetu przyczynił się jednak zdecydowanie bardziej projekt World Wide Web. Został on zapoczątkowany w 1989 roku w CERN przez Tima Bernersa-Lee. Oparty na hipertekstowości (HTTP — Hypertext Transfer Protocole[20]), był nowatorską i zarazem łatwo dostępną metodą prezentowania danych w formie cyfrowej online. Dzięki tej idei już w 1990 roku powstała pierwsza strona internetowa pod adresem info.cern.ch. To również Europejska Organizacja Badań Jądrowych jako pierwsza w 1991 roku zaprezentowała jednolity standard World Wide Web. Bez wątpienia WWW stało się jednym z tych osiągnięć, które w największym stopniu wpłynęło na popularyzację Internetu. Zdaniem Piotra Gawrysiaka (2008: 245—246) powstanie i rozwój WWW oznaczało dla większości ludzi

> zmianę sposobu postrzegania komputera jako urządzenia wspomagającego pracę umysłową. Mamy tutaj bowiem do czynienia ze zmianą paradygmatu — przejściem od komputera będącego urządzeniem osobistym, swego rodzaju prywatnym repozytorium informacji […] do komputera będącego terminalem łączącym człowieka z systemem globalnym. Rola komputera osobistego zaczyna się zatem zmniejszać — informacja, do której poszukujemy dostępu, a nawet samo przetwarzanie tej informacji, ulokowana jest bowiem w globalnej strukturze WWW i dostępna jest z dowolnego połączonego z nią terminala (Gawrysiak, 2008: 245—246).

W tym kontekście według autora wydarzenie to miało skutki porównywalne z wynalezieniem prasy drukarskiej przez Gutenberga (Ibidem). Natomiast zdaniem Marka Pudełko (2013: 150) sukces WWW wynikał z sześciu czynników: relatywnej prostoty, dużych możliwości technicznych, jasnego sposobu korzystania z własności intelektualnej, zwartego i logicznego systemu funkcjonowania, jednolitego sposobu adresowania oraz braku opłat za korzystanie.

Według Raphaela Cohena-Almagora to właśnie w tym czasie doszło do wejścia Internetu w fazę komercyjną, która w konsekwencji doprowadziła do wykształcenia się jego współczesnej formy. Już nieco wcześniej, wraz z wyod-

[20] Jest to „protokół transmisyjny, który określa zasady interakcji między przeglądarką i serwerem WWW w czasie przesyłania danych". Za: Comer, 2012: 81.

rębnieniem się części wojskowej, nastąpił dynamiczny wzrost liczby użytkowników cywilnych, niezwiązanych już wyłącznie z badaniami naukowymi dla wojska. W 1986 roku liczba użytkowników samego ARPANET-u sięgnęła 5000. W ciągu roku została ona podwojona, co najlepiej świadczyło o szybkości rozwoju tej formy komunikowania. Wraz ze stopniowym wycofywaniem się rządu Stanów Zjednoczonych z tego projektu coraz większe zaangażowanie przejawiał sektor prywatny. W tym czasie doszło do zbudowania szeregu połączeń wykorzystujących protokół TCP/IP między ARPANET-em a innymi funkcjonującymi wówczas sieciami. Zdaniem Cohena-Almagora ważnym wydarzeniem było również wdrożenie nowatorskich połączeń DS-1 o prędkości ok. 1,5 Mb/s, co znacząco przyspieszyło funkcjonowanie globalnej sieci i pozwoliło na przekroczenie w 1988 roku liczby 100 000 podłączonych do niej komputerów (Cohen-Almagor, 2011: 51—52). Symboliczną datą, która zamknęła ten pierwszy, pierwotny etap formowania się Internetu, był z pewnością rok 1990. 28 lutego DARPA oficjalnie zakończyła projekt ARPANET, przekazując wszelkie uprawnienia dotyczące funkcjonowania sieci National Science Foundation. Decyzja ta wynikała przede wszystkim z faktu, iż była ona oparta na przestarzałych rozwiązaniach, przez co nie nadążała za rozwojem innych elementów Internetu. W wyniku tego wydarzenia rdzeniem globalnej sieci stała się więc wspomniana już NSFNet (Pudełko, 2013: 91).

Na tej podstawie warto pokrótce omówić, w jaki sposób postrzegano reperkusje pierwszego stadium rewolucji informatycznej. Jak wspomniano wyżej, już w latach 50. i 60. pojawiły się pierwsze głosy wskazujące na rosnący wpływ rozwoju naukowo-technicznego na szeroko pojęte stosunki społeczne. W kolejnych dekadach opinie te stały się coraz bardziej powszechne. W 1970 roku, czyli jeszcze przed nastaniem ery komputerów osobistych, James Martin oraz Adrian R.D. Norman (1970: 95, 213) pisali np. o powstaniu skomputeryzowanego społeczeństwa w ciągu następnych piętnastu lat, doceniając rolę nowych technologii, np. w edukacji czy ochronie zdrowa. Zbigniew Brzeziński (1970: 10, 19) w tym samym czasie wskazał, iż na świecie, a szczególnie w Ameryce, doszło do nastania nowej ery technotronizmu. Jak twierdził:

> Wpływ nauki i technologii na człowieka i jego otoczenie […] staje się głównym źródłem współczesnej zmiany. […] Transformacja, która ma teraz miejsce, szczególnie w Ameryce, już teraz formuje społeczeństwo coraz bardziej odmienne od jego uprzemysłowionego poprzednika. Społeczeństwo postindustrialne staje się społeczeństwem technotronicznym.

Jego zdaniem technologia i elektronika, a w szczególności komputery oraz komunikacja, dokonały istotnych zmian w życiu człowieka w takich dziedzinach, jak kultura, psychologia czy gospodarka. Jako jeden z pierwszych badaczy zwrócił także uwagę na zjawisko rosnących dysproporcji w zakresie roz-

woju technologicznego i możliwych tego konsekwencji w wymiarze globalnym (Ibidem, s. 10, 19). W tym czasie również wielu innych naukowców pisało o coraz wyraźniejszych zjawiskach występujących na styku technologii komunikacyjnych i informacyjnych (ICT) oraz życia społecznego. Donald M. Lamberton (1974) pisał w tym kontekście otwarcie o rewolucji informacyjnej, natomiast Philip H. Abelson i Allen L. Hammond o rewolucji elektronicznej (1977). Warto także wspomnieć o powstałych w latach 80. XX wieku koncepcjach państwa komputerowego oraz „człowieka Turinga". Twórcą pierwszej z nich był David Burnham (1983: 167), który wskazywał nie tylko na rosnące znaczenie ICT w funkcjonowaniu państwa, ale także na możliwość kontrolowania dzięki nim społeczeństwa. „Człowiek Turinga" Davida J. Boltera był natomiast próbą połączenia humanistycznego i ścisłego podejścia do procesów i przemian zachodzących na styku technologii, kultury i społeczeństwa. Zdaniem badacza coraz powszechniejsze wykorzystanie komputerów zmieniło stosunek Zachodu do takich kwestii, jak przestrzeń, czas, pamięć, logika, język czy kreatywność. W tym ujęciu „człowiek Turinga", znajdujący się pod wpływem technologii ICT, stał się połączeniem idei i wartości starożytnej Grecji i faustowskiego dążenia do potęgi poprzez wiedzę. Według D.J. Boltera „człowiek Turinga" jest więc „najbardziej kompletnym połączeniem humanizmu i technologii, rzemieślnika i artefaktu, w historii kultur zachodnich" (Bolter, 1984: 14; Fulmański, Sobieski, 2004: 22—23). Na tej podstawie w połowie lat 80. coraz częściej zaczęto wykorzystywać pojęcie *społeczeństwa informacyjnego*[21], przez które z reguły rozumiano społeczeństwo rządzone innymi niż dotychczas zasadami. Uznawano, iż głównym czynnikiem wpływającym na przemiany społeczne stała się właśnie informacja. Strategicznym zasobem przestał być kapitał finansowy, stał się nim natomiast kapitał intelektualny. Maszyny, istotne w erze przemysłowej, straciły prymat na rzecz ICT. Generalnie rzecz biorąc, wszystkie te teorie podkreślały znaczenie rozwoju naukowo-technicznego, w tym upowszechnienia komputerów oraz ich sieci jako zasadniczego czynnika wpływającego na wzrost gospodarczy i rozwój społeczny. Jednocześnie pojawiały się jednak głosy, które wskazywały, iż początkowe stadium rewolucji informatycznej nie stało się, wbrew oczekiwaniom, dostatecznym remedium na najpoważniejsze problemy globalne, zarówno w wymiarze gospodarczym, społecznym, jak i politycznym (Kenway, Bullen, Fahey, Robb, 2006: 9—19).

Koncepcje powstałe w latach 70. i 80. XX wieku z pewnością posiadały kilka cech wspólnych. Przede wszystkim wskazywały na rosnącą rolę technologii (tele)informatycznych w życiu społecznym. Po drugie zgadzały się w większości co do tego, że sprzyjają one rozwojowi gospodarczemu, naukowemu oraz

[21] Sam termin pojawił się po raz pierwszy w Japonii, został zaproponowany w 1963 roku przez Tedao Umesamo, a w pięć lat później został spopularyzowany przez Kenichi Koyamę. Istnieje wiele różnorodnych definicji *społeczeństwa informacyjnego*, które kładą nacisk przede wszystkim na kategorię *informacji*.

społecznemu. Po trzecie wreszcie wedle tych koncepcji wpływy technologii ICT przejawiały się również w wymiarze kulturowym, tworząc zręby nowego typu człowieka, jakościowo odmiennego od modelu charakterystycznego dla ery przemysłowej. Trafnie diagnozując pewne ogólne trendy właściwe dla początkowej fazy rewolucji informatycznej, koncepcje te jednak tylko w niewielkim stopniu skupiły się na konkretnych przejawach przemian oraz związanych z nimi potencjalnych wyzwaniach. Wynikało to przede wszystkim z faktu, iż postęp naukowo-techniczny w tej dziedzinie, jakkolwiek nabierał rozpędu, nie osiągnął wówczas swoistej „masy krytycznej". Osiągnięcia na obszarze ICT stawały się co prawda coraz bardziej popularne w państwach zachodnich, nie wywierały jednak wyraźnego wpływu na funkcjonowanie państw i społeczeństw. Co więcej, ze względu na rywalizację zimnowojenną procesy te tylko w niewielkim stopniu były obecne w krajach komunistycznych i Trzeciego Świata, należy zatem zauważyć, iż rewolucja informatyczna miała pod koniec lat 80. XX wieku charakter nierównomierny i znajdowała się nadal w początkowym stadium, w którym jej rzeczywisty wpływ na życie społeczne, gospodarcze, kulturowe czy polityczne miał ograniczony charakter.

1.2. Rewolucja informatyczna na przełomie XX i XXI wieku

Drugie stadium rewolucji informatycznej rozpoczęło się na przełomie lat 80. i 90. XX wieku, wpisując się niejako w doniosłe przemiany w środowisku międzynarodowym, związane z upadkiem ładu bipolarnego (Robinson, 1997: 248—260; Rischard, 1997: 268—277; Dunn-Cavelty, 2008: 12). Najdonioślejszą cechą, która odróżniała tę fazę od etapu pierwotnego, było upowszechnienie technologii informatycznych oraz ich globalizacja. W przeciwieństwie do wcześniejszego okresu korzyści wynikające z przełomowych osiągnięć naukowo-technicznych zaczęły być odczuwalne również poza grupą państw rozwiniętych, a ponadto procesy proliferacji komputerów oraz Internetu zaczęły dynamicznie przyspieszać. Tendencje te najlepiej oddają statystyki rozwoju globalnej sieci: w 1989 roku liczba użytkowników Internetu oscylowała w granicach 159 000, obejmując stopniowo już nie tylko Amerykę i Europę, ale również inne kontynenty. Było to możliwe nie tylko ze względu na omówione wyżej osiągnięcia techniczne, lecz także ze względu na zmieniającą się sytuację geopolityczną. Jak wskazano wyżej, jednym z powodów zainicjowania projektu ARPANET była rywalizacja z blokiem państw komunistycznych, upadek układu dwubiegunowego na przełomie lat 80. i 90. XX wieku otworzył więc możliwość ekspansji Internetu do państw, które dotychczas były od niego odseparowane. Najlepiej świadczył o tym fakt, iż już w 1991 roku podłączone zostały do niego

m.in. Chorwacja, Polska, Węgry, Tajwan, RPA oraz Tunezja. W tym czasie sieć zaczęła więc stawać się medium prawdziwie globalnym, w którym ruch osiągnął pułap 10 miliardów pakietów danych przesyłanych każdego miesiąca. Już w rok później liczba użytkowników sieci przekroczyła 1 milion. Co więcej, funkcjonowało wówczas ok. 50 stron internetowych. W 1993 roku ich liczba wzrosła do 623, co świadczyło dobitnie o skali rozwoju tej formy aktywności online (Cohen-Almagor, 2011: 53—54).

Fundamentalny wpływ na ekspansję Internetu miały także dalsze procesy komputeryzacji, w tym przede wszystkim popularyzacja komputerów osobistych (PC), początek lat 90. XX wieku stanowił bowiem czas, kiedy „trafiły one pod strzechy" na całym świecie. Co prawda, jak sygnalizowano wyżej, już zdecydowanie wcześniej pojawiały się takie urządzenia domowe, nie były one jednak na tyle wszechstronne, aby odpowiednio wykorzystać możliwości Internetu. W odróżnieniu od modeli popularnych w latach 70. i 80. PC zdecydowanie ułatwiało nie tylko rozrywkę, ale umożliwiało także zastosowanie rozmaitych zaawansowanych aplikacji użytkowych. Na tym tle do połowy lat 90. Internet przestał być siecią ograniczoną jedynie do państw rozwiniętych. W 1993 roku do sieci szkieletowej podłączone zostały m.in. Bułgaria, Egipt, Kostaryka, Rosja, Turcja oraz Ukraina. Pod koniec tego roku liczba użytkowników wynosiła już 2,1 mln. Co prawda było to niewiele w skali globalnej, dowodziło jednak dynamicznego rozwoju. W tym czasie zaczęły się również pojawiać pierwsze poważniejsze przedsięwzięcia komercyjne, takie jak Yahoo czy sklepy internetowe. W 1994 roku liczba użytkowników wzrosła do 3 milionów, na co wpływ miało także podłączenie do Internetu kolejnych państw: Filipin, Nikaragui, Nigru, Libanu czy Urugwaju. W połowie lat 90. XX wieku usługi internetowe oferowało już ok. 300 dostawców z całego świata, funkcjonowało wówczas już ok. 30 000 stron WWW. Ciekawym zjawiskiem, które większą popularność zyskało właśnie w tym czasie, było Open Source, ruch wolnego oprogramowania, związany zresztą z wytworzoną wcześniej kulturą hakerów. W 1995 roku doszło również do jeszcze jednego, niezwykle istotnego wydarzenia, zdecydowano bowiem o wyłączeniu NSFNet i prywatyzacji sieci szkieletowej. Jak zauważył Raphael Cohen-Almagor (2011: 53—55), to właśnie wówczas Internet stał się punktem łączącym „komunikację, informacje oraz biznes" (zob. też Gawrysiak, 2008: 285—321), natomiast zdaniem Magdaleny Szpunar (2012: 47) Internet wszedł wtedy „w trzeci etap rozwoju, który cechowała komercjalizacja kosztem edukacji". Wszystkie te zmiany doprowadziły do zwielokrotnienia liczby użytkowników sieci, która w grudniu 1995 roku osiągnęła 16 milionów, a w grudniu 1996 aż 36 milionów[22]. Trafnie przemiany te podsumował Manuel Castells (2003: 27), według którego

[22] *Internet Growth Statistics*. Internet World Stats: www.internetworldstats.com/emarketing.htm; dostęp: 24.06.2013.

> w połowie lat dziewięćdziesiątych Internet był sprywatyzowany, jego otwarta architektura pozwalała mu się łączyć ze wszystkimi sieciami komputerowymi na świecie, istniało oprogramowanie pozwalające na właściwe funkcjonowanie WWW, a jego użytkownicy mieli do dyspozycji kilka wygodnych w obsłudze przeglądarek sieciowych. Choć Internet narodził się w umysłach informatyków na początku lat sześćdziesiątych […], to dla większości zwykłych ludzi i świata biznesu Internet narodził się w 1995 roku.

W wyniku omówionych wyżej procesów w drugiej połowie lat 90. XX wieku rewolucja informatyczna zaczęła osiągać swą dojrzałą formę. Można tu wymienić kilka przykładów tego stanu rzeczy. Przede wszystkim zaczęły się powszechniej pojawiać wyizolowane sieci zwane „intranetami". Działając na tej samej zasadzie co ich wersja globalna, były one z reguły wykorzystywane przez instytucje państwowe i sektor prywatny. Powstały też pierwsze wyszukiwarki internetowe, niezbędne w sytuacji, w której lawinowo rosła ilość danych oraz uczestników online. Do przełomowego wydarzenia doszło w 1997 roku, kiedy rozpoczęto projekt FLAG (Fiber-Optic Link Around the Globe), polegający na stworzeniu sieci długich na ponad 27 000 kilometrów światłowodów, których zadaniem było podłączenie całego świata do szybkiego Internetu. To właśnie dzięki tej inicjatywie stał się on medium prawdziwie globalnym, projekt doprowadził bowiem do zarejestrowania w ciągu tylko jednego roku aż 50 nowych domen państwowych. W wyniku tych przemian grudniu 1997 roku do Internetu miało już dostęp 1,7% populacji globu, czyli ok. 70 mln ludzi. W rok później było to aż 147 milionów. W połowie 1998 roku w sieci działało 1,3 mln stron internetowych. W grudniu 1999 roku 4% ludzkości (ok. 248 milionów) mogło korzystać z zasobów znajdujących się online[23]. Doszło też do dalszego przyspieszenia rozwoju technologii komputerowych, prace w tej dziedzinie nie skupiały się jednak wyłącznie na podniesieniu mocy obliczeniowej, lecz także na osiągnięciu coraz większej elastyczności i użyteczności nowych urządzeń i aplikacji. W połowie lat 90. XX wieku korporacja Microsoft wypuściła np. na rynek przeglądarkę Internet Explorer, która przez następne lata rywalizowała z programem Netscape Navigator (Pudełko, 2013: 152—157). Wynikiem tych wysiłków było coraz szersze wykorzystanie ICT nie tylko przez środowisko naukowe, wojsko czy sektor prywatny, ale także w coraz większym zakresie przez sektor publiczny. Potencjał drzemiący w teleinformatyce został w końcu dostrzeżony przez urzędy i służby państwowe na całym świecie. Pojawiły się nowe, niespotykane wcześniej sposoby zastosowania potencjału Internetu. Z jednej strony zaczął być on wykorzystywany jako medium umożliwiające nowe i wyjątkowe w swojej istocie kontakty społeczne: służyły temu m.in. kanały IRC, fora dyskusyjne czy pierwsze blogi; z drugiej — stał się również narzędziem roz-

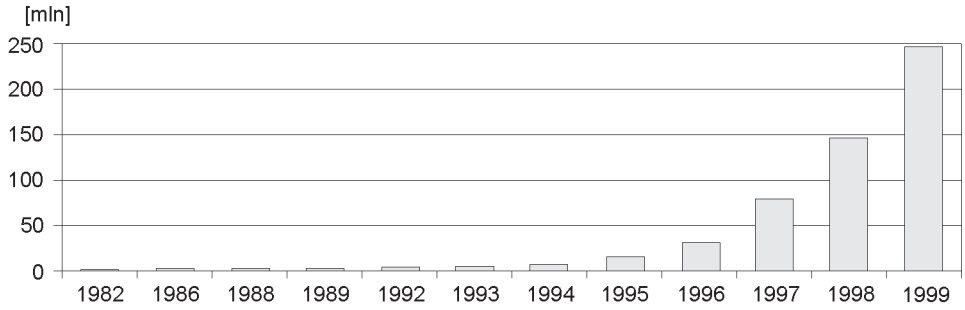
[23] Cohen-Almagor, 2011: 53—55; *Internet Growth Statistics*. Internet World Stats: www.internetworldstats.com/emarketing.htm; dostęp: 24.06.2013.

rywki[24] oraz edukacji dla milionów użytkowników komputerów osobistych. Towarzyszyła temu nieustająca ekspansja nowatorskich przedsięwzięć komercyjnych online (Lakomy, 2013: 42—43). Warto zwrócić również uwagę na zmieniający się sposób zarządzania globalną siecią. Początkowo rozwój ARPANET-u był kontrolowany przez agencje ARPA/DARPA. Standardy techniczne, takie jak protokoły TCP/IP, wyznaczała wówczas Network Working Group. Nieco później powołano Internet Configuration Control Board (ICCB) złożony ze specjalistów pracujących nad poprawą technicznych standardów funkcjonowania sieci. W 1984 roku powstał Internet Activities Board (IAB), który zgromadził najbardziej uznanych specjalistów zajmujących się teleinformatyką. Gdy IAB rozrosła się do kilku tysięcy osób, w 1989 roku została rozdzielona na Internet Engineering Task Force (IETF) oraz Internet Research Task Force (IRTF). Pierwsza z nich zajmowała się głównie bieżącymi usprawnieniami technicznymi, druga natomiast długofalowym planowaniem rozwoju Internetu. Wyniki prac obu tych grup nie miały nigdy charakteru wiążącego, były jedynie zestawem nieformalnych standardów. Wraz z dojrzewaniem decyzji o prywatyzacji sieci w 1992 roku zdecydowano o powołaniu Internet Society (IS): organizacji, która miała nadzorować wszystkie powołane wcześniej gremia. Wraz z globalizacją Internetu do IS przyjęto znaczną liczbę ekspertów z całego świata, co pozwoliło na zinternacjonalizowanie wysiłków na rzecz jego rozwoju. Warto wspomnieć o powołanej przez rząd Stanów Zjednoczonych w 1988 roku Internet Assigned Numbers Authority. Została ona stworzona w celu przydzielania adresów internetowych. W 1998 roku zdecydowano o jej przekształceniu w pozapaństwową, prywatną organizację globalną — Internet Corporation for Assigned Names and Numbers (ICANN), co nastąpiło ostatecznie pod koniec 2000 roku. Zlecono jej takie zadania, jak przydzielanie adresów IP, ustalanie parametrów protokołów i zarządzanie nazwami domen (Castells, 2003: 39—45).

Na tej podstawie można więc stwierdzić, iż w drugiej połowie lat 90. XX wieku Internet stracił swój pierwotny, ekskluzywny charakter. Pod koniec poprzedniej dekady był on nadal domeną głównie użytkowników związanych w jakimś stopniu ze środowiskiem naukowym, wojskiem lub sektorem prywatnym, stopniowo jednak dzięki upowszechnianiu komputerów PC oraz nowatorskim rozwiązaniom technologicznym (World Wide Web, Internet Relay Chat, FLAG) sieć zaczęła stawać się medium w coraz większym stopniu globalnym.

W tym kontekście warto zauważyć, iż do kolejnego przełomowego wydarzenia doszło na początku XXI wieku, kiedy nastąpiło pęknięcie tzw. bańki

[24] Na rosnące znaczenie rozrywki jako elementu rewolucji informatycznej zwrócili uwagę m.in. Hundley, Anderson, Bikson, Neu, 2003: 15—16.



Wykres 1. Liczba użytkowników Internetu w latach 80. i 90. XX wieku (w mln)

Źródło: opracowanie własne na podstawie: Cohen-Almagor, 2011: 53—55; *Internet Growth Statistics*. Internet World Stats: www.internetworldstats.com; dostęp: 24.06.2013.

internetowej[25]. Kryzys wynikający z przeceniania możliwości biznesu sieciowego doprowadził od maja 2000 roku do serii bankructw oraz kryzysu giełdowego (Castells, 2003: 44—45). Udowodniło to, iż bez względu na ogromne korzyści wynikające z rewolucji informatycznej pojawiały się na tym tle również potencjalne i realne wyzwania. Zbiegło się to w czasie z innym doniosłym procesem, którym było wyodrębnienie się tzw. Web 2.0. Charakteryzował się on zmianą dominującego dotychczas modelu wykorzystania sieci przez użytkowników w sposób bierny, który polegał przede wszystkim na zastosowaniu istniejących już narzędzi i aplikacji (np. WWW czy IRC). Tymczasem od przełomu milenijnego internauci coraz aktywniej zaczęli sami współtworzyć zawartość sieci, dzieląc się z innymi własnymi osiągnięciami. Pojawiły się nowatorskie, wcześniej niespotykane sposoby użytkowania istniejących już technologii, czego najdonioślejszym symbolem stały się media społecznościowe. Do najpopularniejszych należy zaliczyć m.in. YouTube, Facebook[26] oraz Twitter. Globalnym zjawiskiem okazał się również rozwój rozrywki online, w tym cieszących się ogromną popularnością gier MMO (Lakomy, 2013: 47—49). Jak stwierdziła Magdalena Szpunar (2012: 57), „zwrócono zatem uwagę na znaczące przesunięcie — od biernego użycia w stronę zaangażowania użytkowników, dzielenia się treścią i danymi, i tworzenia się społeczności online wokół serwisów społecznościowych". Natomiast według Marka Pudełko (2013: 216) było to „otwarcie Internetu na internautów — ich potrzeby i możliwości". Na tym tle pojawiły się równolegle głosy wskazujące na zbyt dużą rolę sieci w życiu jednostek. Dimi-

[25] Był to, jak określił Marek Pudełko (2013: 175—209), okres hossy na światowych giełdach, wywołanej nieuzasadnionym optymizmem, jeśli chodzi o funkcjonowanie sektora IT.

[26] Facebook stał się bez wątpienia najpopularniejszym serwisem społecznościowym na świecie. W 2012 roku liczba jego użytkowników przekroczyła 1 miliard. Zob. *Facebook tops 1 bilion users*. USA Today, 04.10.2012: www.usatoday.com/story/tech/2012/10/04/facebook-tops-1-billion-users/1612613; dostęp: 17.07.2013.

tri A. Christakis (2010) pisał wręcz, iż rosnące uzależnienie użytkowników od Internetu może stać się „epidemią XXI wieku".

Omówione wyżej przemiany, przyczyniając się do dalszej popularyzacji sieci oraz technologii komputerowych, zmieniły charakter samej rewolucji informatycznej, jednym z głównych rezultatów pojawienia się Web 2.0 było bowiem zainteresowanie się ICT przez te grupy społeczne, które dotychczas z tego typu narzędzi nie korzystały bądź robiły to rzadko. Serwisy, takie jak Facebook, zaczęły być używane masowo, przez osoby w różnym wieku, o rozmaitym statusie społecznym i zainteresowaniach. Pozwoliło to branży IT na wyjście z zapaści finansowej, generowało bowiem zapotrzebowanie na nowe, bardziej elastyczne i przystosowane do zmieniających się wymagań urządzenia i aplikacje.

Warto wskazać na kilka przykładów, które świadczyły o dynamicznym postępie w tej dziedzinie na początku XXI wieku. Przede wszystkim przejawiało się to dalszym wzrostem mocy obliczeniowej, a co za tym idzie możliwości komputerów. Rosnąca szybkość procesorów, bardziej efektywne karty graficzne oraz pojemniejsze pamięci RAM pozwalały na wykonywanie działań, które jeszcze dekadę wcześniej były zaliczane do wizji rodem z literatury fantastyczno-naukowej. Komputery stały się zatem urządzeniami zdecydowanie bardziej elastycznymi i wielofunkcyjnymi. W tym kontekście można zauważyć, iż tempo rozwoju branży IT zaskoczyło samych jej twórców. W 1977 roku Ken Olsen twierdził, iż nie ma i nie będzie potrzeby posiadania komputera domowego, w kilka lat później Bill Gates zadeklarował natomiast, iż 640 KB pamięci powinno wystarczyć każdemu[27]. W świetle osiągnięć pierwszej dekady XXI wieku opinie te okazały się zupełnie chybione.

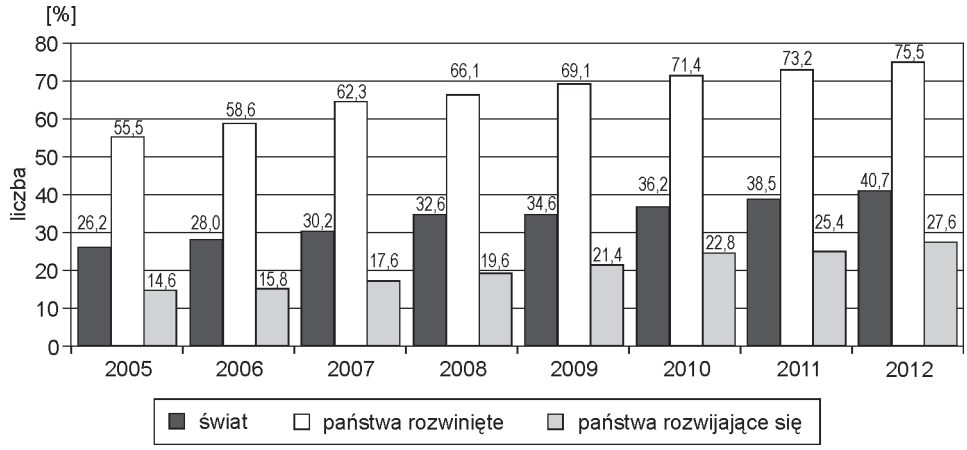
Po drugie: nastąpiło przyspieszenie procesów komputeryzacji. Według raportu korporacji Gartner z 2008 roku liczba funkcjonujących wówczas na świecie komputerów sięgnęła zawrotnej liczby 1,1 mld jednostek. Dawało to przeciętny poziom 165 urządzeń tego typu na 1 000 mieszkańców globu. Według raportu do 2014 roku liczba ta miała się podwoić[28]. O tym, jak duże zmiany nastąpiły na tym obszarze, mogły świadczyć również wyniki sprzedaży: w 2001 roku sprzedano bowiem ok. 125 milionów komputerów, dla porównania w 1977 było to jedynie 48 000[29].

---

[27] H. Wallop: *Bill Gates and Sir Alan Sugar made some of worst technology predictions of all times*. „The Telegraph", 09.12.2008: www.telegraph.co.uk/technology/3690203/Bill-Gates-and-Sir-Alan-Sugar-made-some-of-worse-technology-predictions-of-all-time.html; dostęp: 28.06.2013.

[28] Zob. *Gartner Says More Than 1 Billion PCs In Use Worldwide and Headed to 2 Billion Units by 2014*. Gartner, 23.06.2008: www.gartner.com/newsroom/id/703807; dostęp: 1.07.2013.

[29] M. Kanellos: *PCs: More than 1 bilion served*. CNET, 30.06.2002: http://news.cnet.com/2100-1040-940713.html; dostęp: 1.07.2013; *Computers Reach One Bilion Mark*. BBC News, 01.07.2008: http://news.bbc.co.uk/2/hi/science/nature/2077986.stm; dostęp: 1.07.2008.



Wykres 2. Gospodarstwa domowe posiadające komputer (w %)
Źródło: opracowanie własne na podstawie: *World In 2013. ICT Facts and Figures*. International Telecommunication Union 2013.

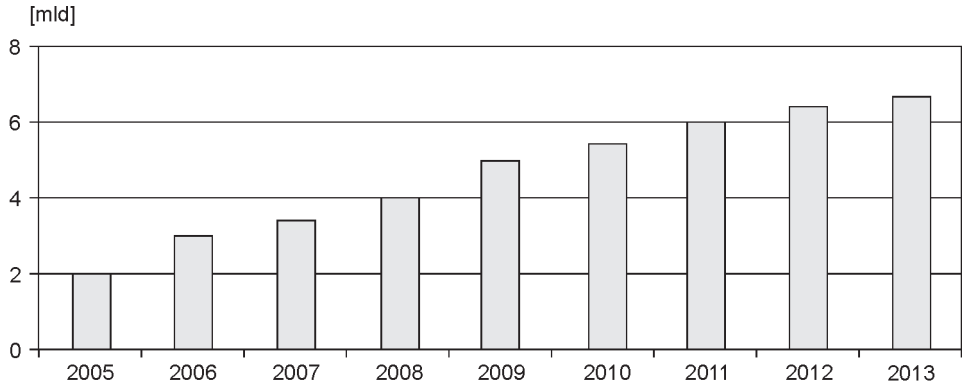
Kolejną istotną zmianą, która nastąpiła na początku XXI wieku, był bezprecedensowy rozwój urządzeń przenośnych. Z jednej strony coraz powszechniej zaczęły być stosowane komputery typu laptop, notebook, palmtop, co wiązało się głównie z ich spadającą ceną i większą przydatnością do codziennej pracy. O zaistnieniu takiej tendencji najlepiej świadczył fakt, iż po raz pierwszy w historii w 2008 roku liczba sprzedanych notebooków w Stanach Zjednoczonych przekroczyła liczbę sprzedanych komputerów typu desktop[30]. Z drugiej strony doszło do rewolucji w zakresie telefonii komórkowej. Telefony komórkowe w pierwszej dekadzie XXI wieku uzyskały dostęp do Internetu, pierwsze bardziej skomplikowane aplikacje użytkowe, programy rozrywkowe czy — z czasem — nawet możliwość wyświetlania filmów. Owocem tego postępu stały się smartfony, będące urządzeniami wielofunkcyjnymi, łączącymi w sobie cechy komputera, telefonu, aparatu fotograficznego, kamery czy telewizora. Rozwiązania tego typu cieszą się ogromną popularnością wśród odbiorców, którzy byli i są zainteresowani mobilnym, szybkim i sprawnym dostępem do globalnej sieci. Tylko w 2012 roku na całym świecie sprzedano aż 821 milionów smartfonów oraz tabletów[31]. Samych popularnych iPhone'ów firmy Apple kupowano ok. 378 000 sztuk każdego dnia[32]. Dla porównania w tym samym czasie sprzedano

[30] *Notebook sales surpass PCs for the first time in US*. AFP, 29.10.2008: http://afp.google.com/article/ALeqM5hkYOf_SCQ1ugSXKLXCsSs7qWnsQA; dostęp: 1.07.2013.

[31] *Miliard nowych smartfonów i tabletów w 2013 r.*, Forbes.pl, 06.11.2012: www.forbes.pl/artykuly/sekcje/techno/miliard-nowych-smartfonow-i-tabletow-w-2013-r-,31089,1; dostęp: 1.07.2013.

[32] *Mobile Stats. Bringing Statistics to Life*. MobileStatistics.com: www.mobilestatistics.com; dostęp: 25.07.2013.

tylko nieco ponad 148 milionów komputerów stacjonarnych[33]. Omówionym wyżej procesom sprzyjał również coraz szybszy rozwój sieci typu Wi-Fi oraz Internetu bezprzewodowego, udostępnianego przez operatorów telefonii komórkowej[34]. Telefony przenośne przestały być zatem jedynie narzędziami służącymi do komunikacji głosowej. Według Piotra Gawrysiaka (2008: 276—277) doszło tu do konwergencji funkcjonalności, „która jest wynikiem potrzeb użytkowników pragnących nosić przy sobie jak najmniejszą liczbę urządzeń". Przejawia się ona głównie w dwóch dziedzinach: rozrywki oraz dystrybucji treści.



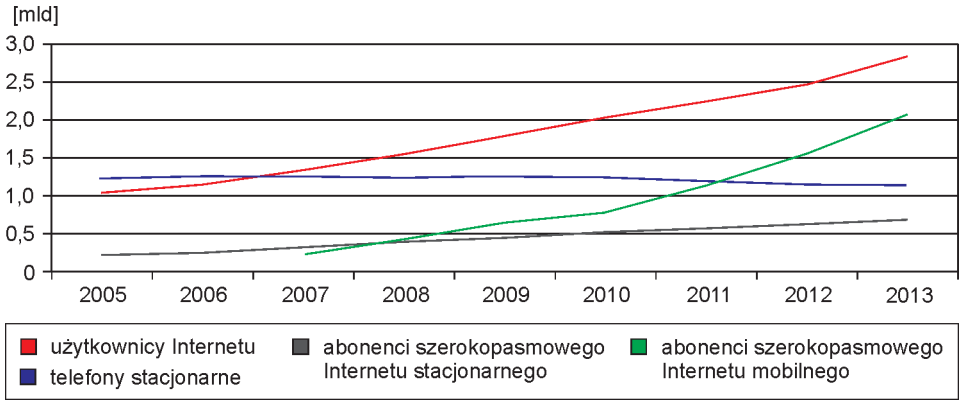
Wykres 3. Liczba użytkowników telefonów komórkowych w XXI wieku (w mld)

Źródło: opracowanie własne na podstawie: *World In 2013. ICT Facts and Figures*. International Telecommunication Union 2013, s. 1.

Na koniec warto zobrazować, jak na tym tle rozwijał się sam Internet. W 2001 roku do sieci podłączonych było ok. 100 mln komputerów (*host*), co przekładało się w skali całego świata na ok. 513 mln użytkowników. W ciągu następnych czterech lat liczba komputerów podłączonych do sieci wzrosła o ok. 500%, tymczasem liczba użytkowników podwoiła się — do 1,018 mld osób w grudniu 2005 roku. W grudniu 2007 roku dostęp do sieci miało już 1,319 mld osób. W latach 2007—2009 liczba ta wzrosła o kolejne pół miliarda. W grudniu 2012 roku internautów było już niemal 2,5 mld. W marcu 2013 według danych Międzynarodowego Związku Telekomunikacyjnego z Internetu korzystało regularnie aż 2,749 mld użytkowników, co stanowiło ok. 39% mieszkańców globu. Co niezwykle ważne, rozwój Internetu w XXI wieku miał charakter nie tylko ilościowy, ale również jakościowy, w pierwszej dekadzie upowszechniły się

[33] N. Lomas: *IDC: Tablet Sales Grew 78.4% YoY In 2012 — Expected To Pass Desktop Sales in 2012, Portable PCs In 2014*. Techcrunch, 27.03.2013: http://techcrunch.com/2013/03/27/idc-tablet-growth-2012-2017; dostęp: 12.08.2014.

[34] *Smartphone*. PCMag Encyclopedia: www.pcmag.com/encyclopedia/term/51537/smartphone; dostęp: 1.07.2013.



Wykres 4. Rozwój telekomunikacji w XXI wieku (w mld)

Źródło: opracowanie własne na podstawie: *World In 2013. ICT Facts and Figures*. International Telecommunication Union 2013.

bowiem łącza szerokopasmowe, które zastąpiły dominujące jeszcze w latach 90. XX wieku modemy telefoniczne[35].

Na tej podstawie można więc zauważyć, iż rozwój technologii informacyjnych i komunikacyjnych od lat końca 90. XX wieku posiadał trzy zasadnicze cechy. Pierwszą była niespotykana do tej pory na taką skalę masowość. Komputer i Internet stały się narzędziami stosowanymi powszechnie w życiu codziennym zarówno w sektorze prywatnym, jak i publicznym. Świadczył o tym najdobitniej fakt, iż dostęp do sieci w 2013 roku miała ponad 1/3 ludzkości, w porównaniu do lat 70. i 80. XX wieku był to więc ogromny postęp[36]. Po drugie: rozwój technologii komputerowych nie był ukierunkowany już tylko na uzyskiwanie coraz wyższych mocy obliczeniowych[37], ale także na użytkowość

[35] Pojawiły się również nowe technologie dostępu do Internetu, w tym m.in. łącza abonenckie, ISDN, technologie cyfrowych linii abonenckich (DSL), łącza ADSL czy światłowodowe technologie dostępowe. Zob. *Internet Growth Statistics*. Internet World Stats: www.interneworldstats.com/emarketing.htm; dostęp: 1.07.2013; *Measuring the Information Society*, 2012; Comer, 2012: 222—230.

[36] Warto w tym kontekście przypomnieć trafność planu Yoneji'ego Masudy, który wyodrębnił w 1972 roku cztery fazy przeobrażania sfer życia społecznego poprzez rozwój technologii informacyjnych i komunikacyjnych. Wyróżnił on: okres komputeryzacji wielkiej nauki (1945—1950), okres komputeryzacji zarządzania (1950—1970), komputeryzacji informacji społecznej (1970—1980) i okres komputeryzacji działań jednostkowych (1980—2000). Za: Goban-Klas, Sienkiewicz, 1999: 44.

[37] David S. Alberts, Daniel S. Popp i W. Thomas Kemp III (1997: 36) wyróżnili 8 najistotniejszych ich zdaniem osiągnięć przyczyniających się do rewolucji informatycznej: zaawansowane półprzewodniki, zaawansowane komputery (*advanced computers*), światłowody, telefony komórkowe, technologia satelitarna, zaawansowane sieci (*advanced networking*), ułatwione interakcje człowiek — komputer oraz cyfrowa kompresja i cyfrowa transmisja danych.

i wielofunkcyjność. Komputer podłączony do sieci stał się dzięki temu nie tylko narzędziem przydatnym do pracy, ale także do nabywania wiedzy, komunikowania czy szeroko pojętej rozrywki. Należy zwrócić również uwagę na pojawienie się nowych „bram" dostępu do sieci. W latach 90. XX wieku jedynym popularnym punktem styku człowieka z Internetem był komputer stacjonarny, dekadę później pojawiła się cała gama innych urządzeń (telefony komórkowe, tablety, telewizory czy nawet zegarki), które to umożliwiały, co wpłynęło w zasadniczym stopniu na charakter rewolucji informatycznej.

1.3. Istota i implikacje rewolucji informatycznej

Alvin Toffler, obserwując coraz szybszy rozwój technologii komputerowych, wysunął w 1980 roku koncepcję „trzeciej fali" (*Third Wave*). Została ona ufundowana na przeświadczeniu, iż ludzkość przeszła dotychczas dwie rewolucje techniczne, z których każda w znacznym stopniu wyeliminowała wcześniejsze kultury i cywilizacje, zastępując je nowym *mode de vie*. Rewolucje te Toffler określił mianem *fal*. Pierwsza, jego zdaniem, obejmowała rewolucję rolniczą i trwała tysiące lat, zanim w pełni ukształtowała nowe oblicze społeczeństwa. Druga wiązała się z początkiem rewolucji przemysłowej i trwała ok. 300 lat. Według autora w drugiej połowie XX wieku nastąpiła trzecia fala, która miała „rozbić nasze rodziny, rozkołysać naszą gospodarkę, sparaliżować systemy polityczne, roztrzaskać nasze wartości" (Toffler, 1980: 10). Mając na uwadze wizję Tofflera oraz omówione wyżej procesy technologiczne, warto więc spróbować odpowiedzieć na pytanie, czym stała się w rzeczywistości rewolucja informatyczna oraz jakie są jej najistotniejsze cechy i konsekwencje.

Przede wszystkim należy zauważyć, iż nie ma zgody badaczy co do momentu, który zapoczątkował rewolucję informatyczną. Zdaniem jednych było nim powstanie pierwszego komputera, według innych zdecydowanie istotniejsze znaczenie miało utworzenie sieci ARPANET i związane z nią osiągnięcia naukowo-techniczne. Nie ulega wątpliwości, iż oba te wydarzenia były dwiema jej najważniejszymi przyczynami sprawczymi. Jak wspomniano jednak wyżej, rewolucja informatyczna polegała nie tylko na opracowaniu tych technologii, lecz przede wszystkim na ich upowszechnieniu na ogromną skalę. Przyjmując takie podejście, za jej początek można uznać dopiero przełom lat 60. i 70. XX wieku, kiedy stopniowo osiągnięcia te przestały być wykorzystywane jedynie przez wojsko oraz niewielką część środowiska naukowego[38], ich potencjał

[38] Ten wcześniejszy okres, mający odmienne cechy, bywa czasami nazywany w odróżnieniu od *rewolucji informatycznej* (*informacyjnej*) — *rewolucją naukowo-techniczną*. Część naukowców datuje ją np. na lata 1940—1970. Zob. Šmihula, 2010: 62.

zaczął być natomiast dostrzegany przez podmioty gospodarcze i — z czasem — przez pojedynczych użytkowników (Mahoney, 1988: 113—125). Bez względu na to aż do końca lat 80. XX wieku rewolucja informatyczna nie przyniosła poważniejszych zmian społecznych, kulturowych bądź ekonomicznych w skali świata. Co prawda doszło wówczas do upowszechnienia komputerów osobistych, był to jednak proces ograniczony, zarówno pod względem jakościowym, co wynikało z ich niewielkich możliwości użytkowych, jak i pod względem geograficznym. Tymczasem sieci komputerowe nadal pozostawały głównie domeną wojska, środowiska naukowego, nielicznych podmiotów gospodarczych oraz pasjonatów. Rzeczywistą transformację przyniosło dopiero drugie stadium rewolucji, które rozpoczęło się na początku lat 90. XX wieku: Internet oraz komputery zaczęły być wówczas stosowane powszechnie w niemal wszystkich dziedzinach aktywności człowieka, co wpisało się zresztą w zjawisko postępującej globalizacji.

Postęp naukowo-techniczny doprowadził wówczas do przemian, które reprezentanci różnych dziedzin nauki prorokowali od dekad. Jak zauważył James N. Rosenau (2000: 9—10, 24), rewolucja informatyczna (informacyjna), udostępniając nowe technologie, które przyspieszyły „rozpad czasu i przestrzeni", przyczyniła się do skomplikowania wielu dziedzin ludzkiego życia, wprowadzając aspekt nieliniowości, pewnego chaosu, „odległej bliskości". Ułatwiła tym samym przezwyciężanie tradycyjnych ludzkich ograniczeń. W tym kontekście warto odwołać się do słów Marka Madeja (2009: 20—21), według którego kluczową zmianą, którą przyniosła rewolucja, nie była wcale szybkość przesyłu informacji, lecz „gwałtowny spadek kosztów gromadzenia, przechowywania i transferu informacji, stanowiący pochodną błyskawicznego wzrostu — dzięki stale doskonalonym technologiom informatycznym — możliwości równoczesnego magazynowania i przesyłania coraz większej ilości danych". Podobnie istotę rewolucji informatycznej widział Peter F. Drucker (1998), który dodał do tej listy jeszcze jedno zagadnienie: zmianę sposobu ich prezentowania. Natomiast dyrektor Massachusetts Institute of Technology Nicolas Negroponte, obserwując te procesy, stwierdził, iż współcześnie dokonuje się przejście od transportu atomów do przesyłania bitów. Jest to możliwe, jak zauważyli Tomasz Goban-Klas oraz Piotr Sienkiewicz, dzięki rosnącej digitalizacji kodowania form informacji. Ich zdaniem (Goban-Klas, Sienkiewicz, 1999: 32, 49)

> o tym, że nastąpiła rewolucja informatyczna, świadczą nie tylko dane i wskaźniki techniczne (np. dotyczące komputerów, systemów telekomunikacyjnych, w tym satelitarnych, urządzeń powielających informacje, a także różnego rodzaju specjalistycznych systemów informatycznych), ale także ekonomiczne analizy rozwoju społeczno-gospodarczego krajów rozwiniętych. Rosnąca ilość informacji oraz wzrost jej dostępności dla obywateli to obecnie wyraźny trend

> w procesie rozwoju społecznego. Tworzą się „społeczeństwa bogate w informacje", których cechy są zasadniczo odmienne od „społeczeństw bogatych w zasoby materialne" i opierających swoją gospodarkę na eksploatacji tych zasobów.

Nieco inaczej zapatruje się na te zagadnienia Piotr Gawrysiak, którego zdaniem istotą tej rewolucji nie było wcale ułatwienie dostępu do informacji, lecz zmiana jej natury. W jego opinii „traktowana przez stulecia na równi z innymi dobrami materialnymi, w ostatnich zaś latach stająca się towarem najcenniejszym, już niedługo przestanie być traktowana w ogóle jako towar, czyli coś, co można kupić i sprzedać". W porównaniu z rewolucjami przełomu XIX i XX wieku „różnica polega jednak na tym, iż w tym wypadku owa produkcja przenosi się w sferę dóbr niematerialnych, zaś same produkty stają się jednocześnie owymi środkami produkcji" (Gawrysiak, 2008: 22, 25).

W ciekawy sposób ujął te kwestie również Krzysztof Liedel (2011: 47—48), wyróżniając szereg elementów, które jego zdaniem cechują proces transformacji ku społeczeństwu informacyjnemu:

1. Informacja stała się podstawowym zasobem strategicznym, od którego zależy stan i organizacja światowej gospodarki.
2. Rozwój technologii informacyjnej dostarcza niezbędnej infrastruktury do przetwarzania i rozpowszechniania informacji.
3. Rynki w coraz większym stopniu mają charakter elektroniczny; ponadto wiedza i informacja stają się obiektami kupna-sprzedaży.
4. Zanikły tradycyjne granice organizacji.
5. Rozwój mediów i usług wyszukiwania informacji przebudował światowy system finansowy.
6. Informatyzacja integruje gospodarki lokalne ze światową.
7. Zacierają się granice między rozrywką a informacją.

Na podstawie powyższych rozważań warto spróbować wskazać na najistotniejsze cechy i konsekwencje rewolucji informatycznej. Przede wszystkim należałoby zwrócić uwagę na jej najbardziej oczywisty wymiar naukowo-techniczny. Powstanie Internetu oraz komputerów w stopniu wcześniej niespotykanym przyspieszyło procesy badawcze w różnych obszarach wiedzy. ICT nie tylko umożliwiły prowadzenie pełniejszego, efektywniejszego i bardziej transparentnego dyskursu, lecz także zrewolucjonizowały same przedsięwzięcia naukowe. Dzięki rewolucji informatycznej pojawiły się wręcz nowe obszary badań i innowacji. Według Tomasza Gobana-Klasa i Piotra Sienkiewcza (1999: 62) do największych przełomów technologicznych może dojść m.in. w biocybernetyce, technice genetycznej, procesach recyklingu, technologiach magazynowania energii, syntezie termojądrowej, mikroelektronice i optoelektronice, robotyce, a także — co naturalne — w samej teleinformatyce. Rewolucja ta przyczyniła się więc do zastosowania nowych technologii nie tylko do badań związanych z rozwojem

militarnym, ale także innych przedsięwzięć naukowych właściwych zarówno dla nauk przyrodniczych, jak i społecznych.

Po drugie warto zwrócić uwagę na wyraźny kontekst komunikacyjny. Jak wspomniano wyżej, podstawową motywacją, która stała za przedsięwzięciem ARPANET-u w latach 60. XX wieku, była chęć ułatwienia wymiany informacji, początkowo między środowiskiem naukowym, później również między innymi grupami użytkowników. W ciągu kilku dekad wykształciła się cała gama narzędzi, aplikacji i usług, które ułatwiły w zasadniczym stopniu nie tylko błyskawiczne porozumiewanie się na wielkie odległości, ale również przesyłanie dużych pakietów danych. Stanowiło to więc swoistą „kompresję czasu i przestrzeni" (Stępień, 2012: 94). Piotr Szeptyński (2014: 82) pisał w tym kontekście o przekształceniu się „globalnej wioski" w „internetową cywilizację". Jak zauważył z kolei Douglas E. Comer (2012: 49), dzięki dostępności wydajnych technik obliczeniowych i komunikacyjnych zmieniło się zastosowanie Internetu, z medium oferującego współdzielenie zasobów stał się bowiem systemem komunikacyjnym ogólnego przeznaczenia. Poczta elektroniczna, USENET, IRC, fora internetowe, World Wide Web czy nawet gry komputerowe w stopniu bezprecedensowym ułatwiły globalną komunikację między rosnącą liczbą użytkowników. Dzięki swojej elastycznej i dynamicznej strukturze sieć umożliwiła nie tylko komunikację porozumiewawczą (użytkownik do użytkownika), lecz także rozsiewczą (jeden użytkownik do wielu) i powszechną (wielu do wielu) (Adamski, 2012: 89). Jak zauważył Andrzej Adamski, Internet stał się „więcej niż tylko medium", ponieważ „globalną sieć można traktować jako nową przestrzeń społeczną, której najistotniejszym społecznym aspektem i celem wykorzystania jest komunikacja". Jego zdaniem Internetu nie da się sklasyfikować na takiej samej zasadzie jak innych mediów, łączy bowiem komunikację masową z indywidualną. Ponadto w sieci mamy do czynienia nie tylko z odbiorcami, ale i aktywnymi użytkownikami (Ibidem, s. 78—83). Warto również przytoczyć opinię Magdaleny Szpunar (2012: 199), która zaprezentowała nieco inne podejście do tego zagadnienia, twierdząc, iż

> po epoce dominacji mediów masowych nowe media miały stać się szansą na realizowanie potrzeb odbiorców wyrugowanych przez dominację gigantów medialnych. Libertariańskie, kontrkulturowe ideały Internetu wydawały się doskonałą podwaliną pod stworzenie medium, które spełniałoby marzenia jednostek o poszerzeniu sfery publicznej i sfery dyskursu, możliwości wyrażania nieskrępowanej i co ważne niezależnej od cenzury opinii.

Jak zauważyła autorka, tak się jednak do końca nie stało, co wynikało m.in. z komercjalizacji Internetu i podążającej za nią organizacji treści w sieci (Ibidem). Bez względu na tę ożywioną debatę należy podkreślić, iż technologie ICT otworzyły wcześniej niespotykane, wyjątkowe w swojej istocie kanały komunikacji, w wielu wymiarach i na wielu płaszczyznach. Stały się one podstawą do

wytworzenia nowej sfery aktywności ludzkiej, w której działalność ma charakter niematerialny i „aterytorialny". W tym kontekście łatwość wymiany informacji oraz jej ogromną skalę należy uznać za podstawowe cechy charakterystyczne rewolucji informatycznej.

Po trzecie: naturalną i oczywistą konsekwencją rewolucji informatycznej stała się powszechność technologii ICT, komputerów oraz sieci (Leszczyńska, 2011: 129; Taddeo, 2012: 210). Jak zauważył Marek Madej (2009: 23):

> rozmaite systemy komputerowe i inne narzędzia elektroniczne są dziś wykorzystywane w każdej gałęzi gospodarki oraz na wszystkich szczeblach struktur państwowych, zaś wynikające z tego powiązania mają charakter transnarodowy. Wszystko to powoduje względną łatwość dostępu przy użyciu narzędzi i technik teleinformatycznych do wielu istotnych danych, informacji i urządzeń, a przez to możliwość oddziaływania nie tylko na procesy zachodzące w samej infrastrukturze teleinformatycznej, ale — co ważniejsze — również w systemach z nią powiązanych.

Współcześnie procesy komputeryzacji i informatyzacji mają miejsce nawet w tak ważnych i wrażliwych obszarach, jak infrastruktura krytyczna[39]. Warto przedstawić to zagadnienie szerzej na przykładzie Polski. W *Strategii kierunkowej rozwoju informatyzacji Polski do roku 2013 oraz perspektywicznej prognozie transformacji społeczeństwa informacyjnego do roku 2020* zauważono, iż „o poziomie rozwoju i miejscu Polski w układzie międzynarodowym, zwłaszcza o pozycji Polski w Unii Europejskiej, w coraz większym stopniu będzie decydować skala dostępności informacji i znaczenie wiedzy. Zależeć będzie od tego konkurencyjność polskiej gospodarki, zarówno w wymiarze ekonomicznym, jak i politycznym". W tym oraz w innych dokumentach rządowych podkreślono więc potrzebę usieciowienia takich dziedzin, jak administracja publiczna, wymiar sprawiedliwości, gospodarka, rolnictwo, nauka, kultura czy bezpieczeństwo (*Strategia kierunkowa*, 2005; *Wyzwania rozwojowe*, 2009). Rzeczywiście te założenia są realizowane, nie tylko w Polsce, ale i na całym świecie, gdzie wprowadza się najnowsze osiągnięcia teleinformatyki jako narzędzia usprawniające funkcjonowanie nie tylko administracji publicznej, ale np. systemów obronnych, finansowych, ochrony zdrowia, komunikacyjnych czy sieci elektroenergetycznych. Należy zatem podkreślić, iż rewolucja informatyczna wiązała się z upo-

[39] Zgodnie z definicją zawartą w *Ustawie o zarządzaniu kryzysowym* z dnia 26 kwietnia 2007 roku rozumie się przez nią m.in. systemy zaopatrywania w wodę, żywność, surowce energetyczne, energię, systemy łączności, finansowe, transportowe, ratownicze czy sieci teleinformatyczne, a więc także „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców". Zob. *Ustawa o zarządzaniu kryzysowym* z dnia 26 kwietnia 2007 roku, Dz.U. z 2007 r., nr 89, poz. 590.

wszechnieniem technologii ICT w różnych sferach funkcjonowania nie tylko jednostek, lecz także społeczeństw, państw oraz ich organizacji[40].

Po czwarte, na co zwrócili uwagę m.in. Richard O. Hundley, Robert H. Anderson, Tora K. Bikson oraz C. Richard Neu (2003: 25—30), fundamentalne przemiany zaszły również w wymiarze ekonomicznym. Najbardziej wyraźnym rezultatem masowego zastosowania komputerów i Internetu było pojawienie się nowych form przedsięwzięć gospodarczych oraz ich większa efektywność, co często określa się mianem e-biznesu. Możliwość szybszego i zarazem tańszego przetwarzania masowych danych skutkowała bardziej dynamicznym dostosowywaniem się do wymagań rynku, podniesieniem konkurencyjności, obniżeniem kosztów produkcji oraz pracy. Teleinformatyka umożliwiła również świadczenie usług na odległość na niespotykaną wcześniej skalę. Stało się to powodem częściowej transformacji w zakresie wymiany towarów i usług na całym świecie (zob. też Šmihula, 2010). Przykładowo już w latach 90. XX wieku pojawił się e-handel, polegający na możliwości zakupu szerokiego asortymentu towarów w sieci bez wychodzenia z domu. Tylko w 2000 roku jego wartość w USA oscylowała w granicach 400 mld dolarów, co najlepiej obrazowało potencjał tego rodzaju przedsięwzięć (Castells, 2003: 77; Atkinson, McKay, 2007; Segal, 1997). Rewolucja informatyczna przyczyniła się również do powstania pieniądza elektronicznego, który współcześnie zastępuje w coraz większym stopniu jego tradycyjną, papierową wersję[41]. Wykształciły się wręcz nowe gałęzie gospodarki, które pełnymi garściami czerpały z możliwości teleinformatyki, nie tylko w zakresie świadczenia różnorodnych usług przez Internet (handel[42], rozrywka[43], komunikacja[44]), lecz także udostępniania samej mocy obliczeniowej komputerów (np. *render farms*). Pojawiły się giełdy elektroniczne oraz usługi bankowe online (Smith Bers, 1997). Ciekawym przykładem zastosowania ICT w gospodarce stał się również tzw. *offshoring*, znany też jako „zdalny *outsourcing*". Polega on na wykorzystaniu komunikacji cyfrowej do wykonywania na odległość zadań zleconych przez firmę znajdującą się w innym miejscu niż pracownik (Gogołek, 2004: 16—17), jest to więc unikalna i wygodna metoda importu siły roboczej. Wreszcie sam sektor IT stał się nową i niezwykle dynamiczną gałęzią gospodarki, jego rozwój przejawia się jednak i w innych dziedzinach m.in. poprzez

[40] Bardzo trafnie materię tę podsumowano w raporcie Microsoftu z 2004 roku, w którym stwierdzono, iż ICT stały się unikalnymi narzędziami, które mogą zostać zastosowane w niemal wszystkich dziedzinach życia społecznego i gospodarczego. Zob. *ICTs as Enablers*, 2004, s. 2—3.

[41] Pierwszym pieniądzem elektronicznym była ECU (*European Currency Unit*), która powstała w 1979 roku. Zob. Pudełko, 2013: 289.

[42] Takie serwisy, jak E-Bay, Amazon, e-Toy. Rynek polski pod tym względem zdominowało Allegro.

[43] Fenomenem XXI wieku stały się m.in. gry MMO czy MOBA.

[44] Pojawiło się wiele nowych programów i usług komunikacyjnych w sieci, w tym np. ICQ, Skype, czaty na stronach WWW.

zaoszczędzenie czasu pracy, zwiększenie wydajności maszyn i urządzeń, polepszenie warunków pracy, skrócenie cyklu produkcyjnego oraz podniesienie jakości wyrobów i usług (Goban-Klas, Sienkiewicz, 1999: 78—79). Potwierdził to zresztą raport Departamentu Handlu USA z 2002 roku, wedle którego inwestycje w nowe technologie miały doniosły wpływ na rozwój ekonomiczny USA na przełomie wieków (*Digital Economy*, 2002). W latach 1995—2010 sektor ICT wypracował aż 25% całego amerykańskiego wzrostu gospodarczego. O znaczeniu tych zagadnień świadczy także fakt, iż w 2008 roku światowy rynek ICT osiągnął zawrotną wartość 3,1 biliona dolarów (Ezell, Andes, 2010: 76—77). Na tej podstawie badacze coraz częściej wskazują na fakt wykształcenia się „globalnej gospodarki informacyjnej" (Drake, 2000: 51).

Warto zauważyć, iż technologie ICT stały się również istotnym czynnikiem sprzyjającym rozwojowi społecznemu. Można tu wskazać na kilka przejawów tego stanu rzeczy. Po pierwsze już w latach 70. i 80. XX wieku sieci komputerowe były wykorzystywane w celach edukacyjnych. Wraz z postępem teleinformatyki zaczęto dostrzegać jej coraz większy potencjał w tej dziedzinie. Z jednej strony wynikało to z umożliwienia użytkownikom Internetu błyskawicznego dostępu do różnorodnych informacji, z drugiej strony zaś połączone ze sobą komputery zaczęły być wykorzystywane również w systemie oświaty, czego najbardziej doniosłym przejawem stał się *e-learning* (Przybycień, 2007; Roszczynialski, 2003; Mehlinger, 1997). Tym samym nowe aplikacje i narzędzia powstałe w wyniku rewolucji informatycznej w zasadniczym stopniu ułatwiły proces zdobywania wiedzy. Zwrócił na to uwagę Manuel Castells, którego zdaniem największym wyzwaniem, które pojawiło się w związku z postępem technologicznym, była zmiana podejścia do edukacji poprzez „utrwalenie się zdolności przetwarzania informacji i wytwarzania wiedzy w każdym z nas, a szczególnie w każdym dziecku" (cyt. za: Hetmański, 2003: 338). Doniosłe zmiany zaszły również w służbie zdrowia: nie tylko pojawiły się nowe urządzenia medyczne oparte na technologiach komputerowych, lecz usprawniono także sam proces świadczenia usług w tej dziedzinie, np. poprzez konsultacje na odległość czy budowanie systemów wymiany informacji o zagrożeniach epidemiologicznych. Nowe technologie okazały się także niezwykle przydatne w wysiłkach na rzecz ochrony środowiska, dzięki nim pojawiły się m.in. skuteczniejsze sposoby monitorowania stanu powietrza czy precyzyjnego wykrywania zanieczyszczeń środowiska naturalnego (zob. *ICTs as Enablers*, 2004: 5—6; Lasoń, Walecki, Trąbka, 2003; Castro, 2009; Coeira, 1997). Warto ponadto zwrócić uwagę na efekty rewolucji informatycznej na obszarze usług społecznych. Dzięki niej możliwe stały się m.in. efektywniejsze zwalczanie bezrobocia, poszerzenie możliwości doboru środków przeciwdziałania ubóstwu, większa skuteczność systemu usług społecznych, stymulowanie samozatrudnienia, podnoszenie aktywności gospodarczej czy poprawa jakości usług świadczonych przez służby społeczne (Szarfenberg, 2004: 71—72).

Na tej podstawie można wskazać na szereg istotnych przemian dotyczących szeroko pojętych stosunków społecznych. Internet oraz technologie komputerowe ułatwiły, jak wskazano wyżej, rozwój komunikacji na poziomie lokalnym, regionalnym czy nawet globalnym, tym samym w zasadniczym stopniu przyczyniły się więc m.in. do dialogu międzykulturowego i międzycywilizacyjnego, zbliżając do siebie odległe dotychczas społeczności ludzkie. Potwierdziło to tezę Marshalla McLuhana, który w 1964 roku pisał, iż „człowiek elektroniczny" będzie „jak pająk przyczepiony w kącie pajęczyny, wyczuwający drgania wszystkich innych pajęczyn" (Goban-Klas, 2003: 33). Globalna sieć ułatwiła ponadto powstawanie nowych rodzajów wcześniej niespotykanych więzi społecznych dzięki unikalnym aplikacjom i usługom, takim jak np. gry online czy media społecznościowe. W tym kontekście za Manuelem Castellsem można zauważyć, iż wykształciła się swoista „kultura Internetu", na którą złożyły się cztery warstwy: kultura techno-merytokratyczna, kultura hakerska, kultura wirtualno-komunitariańska oraz kultura przedsiębiorczości. Wspierają one, zdaniem autora, „powszechną w internetowym świecie ideologię wolności". Pozwoliło to na wykształcenie się nowego rodzaju grup społecznych, tzw. społeczności sieciowych, które „na nowo zdefiniowały pojęcie społeczeństwa". Zdaniem Castellsa Internet „idealnie pasuje do zasadniczych cech charakteryzujących ruchy społeczne ery informacyjnej. Znajdując w sieci odpowiednią dla siebie formę organizacyjną, ruchy te zainicjowały przemiany społeczne, które z kolei wzmocniły pozycję Internetu jako preferowanego przez nie środka przekazu". Według autora wynikało to z trzech powodów. Po pierwsze ruchy te koncentrują się na wartościach kulturowych, po drugie wypełniają lukę po „pionowo zintegrowanych organizacjach" odziedziczonych po erze przemysłowej, po trzecie wreszcie wynika to z globalizacji ruchów społecznych (Castells, 2003: 47—74, 159—162). Na tym tle Richard O. Hundley, Robert H. Anderson, Tora K. Bikson, C. Richard Neu (2003: 49) stwierdzili, iż rewolucja informatyczna ma i będzie miała szeroki wpływ na życie społeczne oraz kulturę, m.in. dzięki erozji cenzury, „przeładowaniu informacyjnemu", demokratyzacji informacji czy wzmocnieniu pozycji jednostki posiadającej dostęp do wiedzy. Część badaczy, w tym np. Piotr Zawojski (2010: 100), pisała wręcz o powstaniu swoistej cyberkultury, będącej specyficznym zestawem praktyki „odnoszących się do posługiwania mediami cyfrowymi w celu tworzenia nowego modelu kultury opartej na synergii tego, co online, z tym, co offline". Zdaniem autora

> w obszarze cyberkultury mamy […] do czynienia zarówno ze zjawiskami artystycznymi, jak i z szeroko rozumianymi strategiami komunikacyjnymi wykorzystującymi nowe, cyfrowe technologie. Uwzględnić też należy rozmaite aspekty wielkiego i stale się powiększającego wpływu nowych technologii (nie tylko komputerowych) na życie codzienne. […] Cyberkultura łączy dwa aspekty: praktyczne dokonania artystów, wynalazców, techników, designerów,

> aktywistów hakerskich etc. oraz wszystkich tych, którzy zajmują się badaniem, opisem, teoretyczną refleksją dotyczącą nowych technokulturowych fenomenów (Zawojski, 2010: 115—116).

Procesy te w rezultacie doprowadziły więc do powstania społeczeństwa informacyjnego, którego zdefiniowanie według Agnieszki Bógdał-Brzezińskiej oraz Marcina Floriana Gawryckiego (2003: 31) jest zadaniem „żmudnym, a szanse na powstanie definicji satysfakcjonującej ogół badaczy są równie nikłe, jak w przypadku pojęcia *globalizacja*. Wynika to z faktu, iż pojęcie to jest »pojemne, a przy tym nieostre i płynne«". W związku z tym warto przytoczyć kilka interesujących prób w tym zakresie. Według Mariana Niezgody (2003: 121—128) społeczeństwo informacyjne wykształciło się w oparciu o cztery sfery: wiedzy i technologii, gospodarki, społeczeństwa i kultury. Do najistotniejszych cech społeczeństwa informacyjnego zaliczył autor: dominację wiedzy, zaawansowaną technologię, dominację sektora usług, globalizację gospodarki, nowe płaszczyzny konfliktów społecznych, nowe typy kontaktów i więzi społecznych (zapośredniczone Internetem), zmieniające się mechanizmy zróżnicowania społecznego czy wreszcie uniwersalizację kultury. Z kolei według Bogumiły Barańskiej (2003: 171) jest to „typ społeczeństwa, kształtujący się w krajach postindustrialnych, w których rozwój technologii osiągnął najszybsze tempo. W społeczeństwie informacyjnym zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności". W Raporcie Bangemanna zauważono, iż „społeczeństwo informacyjne charakteryzuje się przygotowaniem i zdolnością do użytkowania systemów informatycznych, skomputeryzowane i wykorzystujące usługi telekomunikacji do przekazywania i zdalnego przetwarzania informacji" (cyt. za: Bógdał-Brzezińska, Gawrycki, 2003: 33). Wydaje się jednak, iż najpełniej termin ten zdefiniowali Piotr Sienkiewicz oraz Tomasz Goban-Klas. Ich zdaniem jest to społeczeństwo, „które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa". Według autorów związane z tym zmiany obejmują m.in. syntezę dynamicznych, silnie powiązanych systemów społecznych, nowe modele motywacji pracowników, zwrot ku gospodarce ekologicznej, ewolucję wartości czy też narastającą deregulację gospodarek (Goban-Klas, Sienkiewicz, 1999: 43, 62—63). W ciekawy sposób do tych rozważań odniósł się Lech W. Zacher (2003: 108), który zauważył, iż istnieje możliwość rozpoczęcia kolejnego etapu ewolucji, przekształcenia społeczeństwa informacyjnego w społeczeństwo wiedzy. Aby to urzeczywistnić, „potrzebna jest informacja (społeczeństwo informacyjne), którą należy „przekuwać" na wiedzę i następnie umieć ją zastosować (co powinno być cechą społeczeństwa opartego na wiedzy)".

Można także zwrócić uwagę na szereg doniosłych politycznych konsekwencji rewolucji informatycznej. Przede wszystkim nowa platforma komunikacji,

jaką stał się Internet, pozwoliła jednostkom w stopniu zdecydowanie większym niż wcześniej wyrażać opinie o działaniach władz państwowych czy wydarzeniach międzynarodowych. Sieć, w odróżnieniu od tradycyjnych form komunikacji, dała więc obywatelom możliwość pośredniego lub bezpośredniego wpływania na rząd i jego przedstawicieli (Auvinen, 2012). Za trafne należy uznać słowa Agnieszki Bógdał-Brzezińskiej oraz Marcina Floriana Gawryckiego (2004: 84—86), którzy stwierdzili, iż „nowoczesne technologie miały […] doprowadzić do odebrania państwom monopolu na środki masowego przekazu, stały się narzędziem wspierającym procesy demokratyzacji". Wymienili oni kilka cech Internetu, które dowodziły tej roli. Ich zdaniem Internet stał się sferą, gdzie możliwe stało się nieskrępowane wyrażanie własnych opinii. Sieć nie ma ponadto charakteru hierarchicznego, co pozwoliło na przezwyciężenie tradycyjnych ograniczeń geograficznych lub społecznych. Wprowadzenie w niej cenzury jest znacząco utrudnione, rozpowszechniły się w niej także nieoficjalne sposoby dystrybucji wiadomości. Internet pogłębił także funkcję kontrolną sprawowaną przez użytkowników i stał się narzędziem bezpośrednich relacji z administracją rządową. Sieć sprzyja również subsydiaryzacji decyzji administracyjnych, zdaniem autorów pogłębił także procesy wzmacniające społeczeństwo obywatelskie (Ibidem, s. 84—86. Zob. również: *Telecommunications and Democracy*. In: Alberts D.S., Papp D.S., eds., 1997, s. 167—180). W tym świetle szczególnie istotna wydaje się informacyjna rola Internetu, dzięki powszechnemu dostępowi do sieci społeczeństwo uzyskało bowiem nieskrępowaną możliwość zdobywania wiadomości, które mogłyby nie być tak łatwo przekazywane za pomocą mediów tradycyjnych. Wydaje się, iż to właśnie ta funkcja determinuje wykorzystanie technologii ICT do działań politycznych. Z całą mocą potwierdziło się to w trakcie arabskiej wiosny, w protestach, które rozpoczęły się w grudniu 2010 roku, sieć odegrała bowiem fundamentalną rolę, nie tylko jako źródło niezależnych od mediów rządowych danych, ale także jako narzędzie przydatne do organizacji protestów i innych przedsięwzięć politycznych (Lakomy, 2011: 45—54).

W tym kontekście warto również wspomnieć o koncepcjach e-rządu (*e-government*) i e-administracji, mających w zamyśle zbliżyć urzędy państwowe do obywateli za pomocą osiągnięć rewolucji informatycznej (Tchórzewski, Zając, Fronczek, Ostaszewski, 2003: 361—371; Bógdał-Brzezińska, 2009: 169—174; Wytrążek, 2013: 171). Ideę e-rządu można najogólniej ująć jako wykorzystanie ICT przez administrację rządową lub lokalną w celu ułatwienia dostępu do usług publicznych. W niektórych definicjach podkreśla się również możliwość oddziaływania za pomocą Internetu na państwowy proces decyzyjny (Jain Palvia, Sharma, 2007; Horan, Grönlund, 2004: 713—729; Porębski, 2001). Sprzężenie zwrotne między instytucjami państwowymi a siecią i komputerami może się przejawiać w takich kwestiach, jak uzyskiwanie informacji od władz państwowych czy samorządowych, komunikowanie się z ich przedstawi-

cielami, płacenie podatków, wyrażanie opinii czy składanie podań i uzyskiwanie zaświadczeń (Lakomy, 2013: 140—141). Jeśli chodzi natomiast o informatyzację administracji publicznej, to warto się odwołać ponownie do opinii Tomasza Gobana-Klasa i Piotra Sienkiewicza (1999: 110), którzy do wynikających z niej korzyści zaliczyli: wzrost skuteczności decyzji politycznych, wzrost skuteczności działania urzędów państwowych, powstanie zrębów demokracji bezpośredniej, zdobycie lepszego wizerunku przez władze czy lepszą komunikację na linii rząd — społeczeństwo. Na tej podstawie widać więc wyraźnie, iż w wyniku rewolucji informatycznej pojawiły się nowe sposoby komunikacji i oddziaływań w polityce wewnętrznej. Z jednej strony upowszechnienie Internetu umożliwiło w stopniu zdecydowanie większym niż wcześniej dostęp obywateli do informacji, co stanowiło źródło wielu unikalnych przedsięwzięć politycznych. Z drugiej strony proliferacja osiągnięć teleinformatyki stworzyła szansę dla aparatu państwowego, który zyskał nowy sposób wpływania na obywateli (Lakomy, 2013: 347—358).

Wszystkie omówione wyżej zagadnienia trafnie podsumował Krzysztof Liedel (2011: 48—49), który wyróżnił szereg czynników determinujących funkcjonowanie gospodarki i społeczeństwa informacyjnego. Wymienił on następujące kwestie:

- traktowanie informacji jako dobra ekonomicznego i podstawowego zasobu,
- upowszechniony dostęp do technologii informacyjnych, tworzących obecnie różne kanały dystrybucji,
- cyrkulacja różnorodnych kategorii informacji, co implikuje nowe formy demokratyzacji,
- ok. 50% zatrudnionych w sektorze informacyjnym,
- udział sektora informacyjnego w PNB (PKB) w okolicach 50%,
- dominacja sektora informacyjnego w gospodarce,
- warunkowanie przez sektor informacyjny sprawnego funkcjonowania innych sektorów gospodarki,
- specjalny status nauki i edukacji.

Na tym tle widać więc wyraźnie, iż korzyści dla całej ludzkości wynikające ze zmian technologicznych, które rozpoczęły się jeszcze w latach 40. XX wieku, miały rzeczywiście rewolucyjny i wielowymiarowy charakter. Ogromna liczba dziedzin życia społecznego, politycznego, gospodarczego czy kulturowego, szczególnie od lat 90., została diametralnie przemodelowana. W ciągu zaledwie kilku dekad nowe technologie nie tylko pozwoliły na powstanie nowych form więzi i stosunków społecznych, ale przyczyniły się także do efektywniejszego zwalczania wielu patologii. Umożliwiły nowe sposoby komunikacji i oddziaływań politycznych między różnorodnymi podmiotami, zarówno na arenie krajowej, jak i międzynarodowej. Przyczyniły się do powstania nowatorskich przedsięwzięć gospodarczych, które pozwoliły na szybszy rozwój ekonomiczny i podniesienie jakości życia. Doprowadziły również do doniosłych

zmian w wymiarze kulturowym. Trafnie podsumował wszystkie te zagadnienia Manuel Castells (2003: 12):

> w ostatnich dwudziestu pięciu latach dwudziestego wieku zbiegły się trzy niezależne procesy, dając początek nowej strukturze społecznej opartej w przeważającej mierze na sieciach. Procesy te wiązały się z potrzebami gospodarki w zakresie elastycznego zarządzania i globalizacji kapitału, produkcji i handlu, wymaganiami społeczeństw, dla których wolność jednostki i swoboda komunikowania stały się nadrzędnymi wartościami, a także z niezwykłym postępem w komputeryzacji i telekomunikacji, jaki umożliwiła rewolucja w dziedzinie mikroelektroniki. W tych warunkach Internet, technologia znana wtajemniczonym, która zdawała się oferować korzyści jedynie informatykom, hakerom i ruchom kontrkulturowym, stał się kluczem, który otworzył przejście do nowej formy społeczeństwa — sieciowego — a wraz z nim do nowej gospodarki.

Mając to na uwadze, należy jednak podkreślić, iż rewolucja informatyczna przyniosła ze sobą nie tylko same korzyści, lecz również szereg poważnych wyzwań. Jak bowiem stwierdziła Magdalena Szpunar, w literaturze specjalistycznej często występuje tendencja ukazywania tego zjawiska jako urzeczywistnienia pewnej utopii, wyidealizowanego wyobrażenia rzeczywistości społecznej. Pisze ona:

> wydaje się, iż wizja determinizmu technologicznego, chociaż kusząca, nazbyt upraszcza rzeczywistość. Technologia jest bowiem nie tylko narzędziem kształtującym, ale i kształtowanym. To od nas, użytkowników, zależy, w jakim celu będziemy z niej korzystać i jak będziemy zmieniać jej formę i właściwości. Związek technologii i człowieka ma charakter symbiotyczny — obie są od siebie zależne i wzajemnie się kształtują (Szpunar, 2012: 13).

Omawiając te kwestie, Christine Rosen zauważyła wręcz, iż współcześnie rozmawia się o technologii w sposób, który był dotychczas zarezerwowany dla sztuki bądź religii (cyt. za: Szpunar, 2012: 11). Mając na uwadze te zależności, warto więc dokonać próby identyfikacji najpoważniejszych zagrożeń, które pojawiły się wraz z nastaniem ery rewolucji informatycznej.

Przede wszystkim potencjalne wyzwania wynikają z samego faktu uzależnienia wielu dziedzin funkcjonowania państw i społeczeństw od niezawodności różnorodnych urządzeń i usług elektronicznych (Mehan, 2008: 14—15; Suchorzewska, 2013: 157). Ludzkość na początku XXI wieku, czerpiąc korzyści z zastosowania coraz szybciej pojawiających się dobrodziejstw naukowo-technicznych, stała się *de facto* ich zakładnikiem (Eriksson, Giacomello, 2006: 244—245). Zwrócił na to uwagę m.in. Marek Madej, którego zdaniem rewolucji informatycznej towarzyszą rosnące potrzeby pojedynczych użytkowników, społeczeństw, organizacji i państw w zakresie dalszego wykorzystywania ICT.

Według autora stało się to impulsem do poszukiwania kolejnych rozwiązań technologicznych, co z kolei determinuje rosnące uzależnienie tych podmiotów od funkcjonowania infrastruktury teleinformatycznej (Madej, 2009: 22—23). Awaryjność urządzeń wspomagających funkcjonowanie np. systemów infrastruktury krytycznej może stanowić poważne zagrożenie dla zdrowia i życia obywateli (Dunn-Cavelty, 2007). Awaria sieci elektroenergetycznej, systemu finansowego bądź komunikacyjnego stała się możliwa nie tylko w wyniku określonych działań człowieka lub katastrof naturalnych, ale także potencjalnej zawodności technologii ICT.

Warto zwrócić również uwagę na charakter najważniejszego osiągnięcia rewolucji informatycznej, czyli Internetu. Jak wspomniano wcześniej, jego powstanie zostało zdeterminowane głównie potrzebą ułatwienia wymiany informacji pomiędzy ośrodkami naukowymi, we wczesnym stadium prac nad nim nie zwracano zatem szczególnej uwagi na bezpieczeństwo sieci i składających się na nią komputerów. Internet został oparty na otwartej architekturze, która nie została zaprojektowana z myślą o ochronie wrażliwych danych. Ten swoisty „grzech pierworodny" Internetu stał się szczególnie widoczny w jego dojrzałej wersji początku XXI wieku: łatwość dostępu do sieci stała się czynnikiem sprzyjającym wykorzystywaniu luk w zabezpieczeniach[45] przez różnorodnie motywowane podmioty. Otwarta architektura, umożliwiając dynamiczny rozwój Internetu, przyczyniła się więc do powstania szeregu poważnych problemów dla bezpieczeństwa. Co ciekawe, ta zasadnicza słabość współczesnych sieci teleinformatycznych paradoksalnie ma jedną pozytywną cechę, jak bowiem zauważył Marek Madej, większa podatność na tego typu oddziaływania, co jest związane chociażby z „wielością punktów wejścia" oraz liczbą powiązanych ze sobą dzięki sieci elementów struktury społecznej, niekoniecznie musi oznaczać dużą wrażliwość na negatywne następstwa. Zdaniem autora w „systemach złożonych" występuje „wewnętrzna odporność", która wynika z wielości składających się na nie elementów podtrzymujących ich stabilność (Madej, 2009: 23). Innymi słowy rozproszony charakter Internetu sprawia, iż awaria bądź zniszczenie jednego węzła nie oznaczają paraliżu globalnej sieci[46].

Wspomnianemu rosnącemu uzależnieniu państw i społeczeństw od zdobyczy rewolucji informatycznej towarzyszy coraz szybszy wyścig technologiczny. Z jednej strony jest to oczywiście zjawisko pozytywne, które pozwala czerpać coraz większe korzyści z tych procesów, z drugiej jednak strony rosnąca rywalizacja ośrodków badawczych oraz producentów sektora IT może się wiązać z pewnymi zagrożeniami. Otóż przez pośpiech, aby zdążyć przed konkurencją,

[45] Przez *zabezpieczenia* można za Krzysztofem Liderman (2009: 15) rozumieć „elementy osobowe, techniczne, programowe lub organizacyjne wykorzystywane w procesach ochronnych do działań, których celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji oraz elementów systemu teleinformatycznego".

[46] Szerzej na ten temat w rozdziale następnym, poświęconym cyberprzestrzeni.

na rynek częściej mogą być wypuszczane produkty niedopracowane, a przez to posiadające bardzo poważne luki w zabezpieczeniach[47], umożliwiające przygotowanie tzw. *exploitów*[48]. Można tu wskazać przykładowo bardzo popularny smartfon iPhone, którego oprogramowanie, jak się okazało, mogło zostać złamane za pomocą prostej wiadomości tekstowej (SMS)[49]. Innym powodem tego stanu rzeczy jest również stale rosnąca złożoność oprogramowania, w tym np. systemów operacyjnych[50]. Niekontrolowany wyścig technologiczny może się także przejawiać wprowadzaniem innowacji w sposób nie do końca przemyślany bądź sprawdzony. W wielu dziedzinach procesy komputeryzacji i informatyzacji wiążą się z pojawianiem się nowych wyzwań, nie tylko w wymiarze bezpieczeństwa, ale także szerzej: w wymiarze politycznym, społecznym bądź gospodarczym. Od lat np. wskazuje się na rosnące zagrożenie awariami systemów finansowych, co mogłoby pociągnąć za sobą katastrofalne skutki gospodarcze[51]. Ponadto istotne i uzasadnione wątpliwości pojawiają się w związku z wysuwanym od lat pomysłem wprowadzenia możliwości oddawania głosów w wyborach za pomocą Internetu, bez względu na ewentualne korzyści tego typu rozwiązania wiązałyby się bowiem z ogromnym ryzykiem dla ich rzeczywistych wyników[52].

Można także zwrócić uwagę na pewne zagrożenia w wymiarze społeczno-kulturowym. Przede wszystkim, jak wspomniano wcześniej, początek rewolucji informatycznej bywa bardzo często utożsamiany z momentem pojawienia się nowych, unikalnych sposobów wymiany idei, informacji, konfrontowania opinii i wypracowywania społecznego konsensusu. Stanowi to wartość dodaną debaty publicznej. Tymczasem, na co zwraca się coraz częściej uwagę, Internet, a szerzej: technologie informacyjne i komunikacyjne, mogą być również źródłem propagującym różnego rodzaju patologie czy też postawy szkodliwe

[47] Pisali o tym m.in. Rahul Telang i Sunil Wattal, 2007: 545.

[48] Program lub technika wykorzystująca wadliwość lub błędy oprogramowania. Zob. Wilson, 2001.

[49] Mulliner, Miller, 2009; *iPhone Hacks Exposed: The Key Facts*. Mashed: http://mashable.com/2009/07/30/iphone-hack; dostęp 3.07.2013.

[50] *Microsoft Security Bounty Programs*. Microsoft Security Response Center: www.microsoft.com/security/msrc/report/bountyprograms.aspx#; dostęp: 3.07.2013; J.N. Hoover: *Feds Identify Top 25 Software Vulnerabilities*. Information Week Government, 27.06.2011: www.informationweek.com/government/security/feds-identify-top-25-software-vulnerabil/231000504; dostęp: 3.07.2013.

[51] Dawidziuk, Łącki, Stolarski, 2009: 41—61; *Cyber security risks present threat to UK financial system, say growing number of companies*. Out-Law, 18.06.2013: www.out-law.com/en/articles/2013/june/cyber-security-risks-present-threat-to-uk-financial-system-say-growing-number-of-companies; dostęp: 3.07.2013.

[52] Zob. Weldemariam, Villafiorita, Mattioli, 2007: 38—49; M.I. Shamos: *Electronic Voting — Evaluating the Threat*. Computer Professionals for Social Responsiblility: http://cpsr.org/prevsite/conferences/cfp93/shamos.html; dostęp: 3.07.2013; J. Kitkat: *Is e-voting a threat to our democracy?* Computer Weekly: www.computerweekly.com/feature/Is-e-voting-a-threat-to-our-democracy; dostęp: 3.07.2013.

z punktu widzenia interesu społecznego bądź bezpieczeństwa państw. Można tu podać szereg przykładów. Od wielu lat Organizacja Narodów Zjednoczonych podkreśla, iż sieć bywa wykorzystywana zarówno do promocji narkotyków, jak i handlu nimi[53]. Coraz częściej środowisko teleinformatyczne staje się również areną działań różnorodnych grup przestępczych[54]. Wielu autorów wskazuje także na fakt, iż Internet stał się nie tylko przestrzenią wolnej wymiany myśli i idei, ale także obszarem coraz bardziej rozpowszechnionych technik marketingowych w różnych dziedzinach, a czasami wręcz propagandy (Terlikowski, 2009: 103). Sytuacja ta w znacznym stopniu zaburzyła więc jego pierwotną rolę. Można także stwierdzić, iż rewolucja informatyczna, a w szczególności powstanie mediów społecznościowych, wpłynęła negatywnie na tradycyjne więzi międzyludzkie[55]. Pisała o tym m.in. Krystyna Doktorowicz (2003: 59), według której

> współczesne społeczeństwa informacyjne cechuje indywidualizm, decentralizacja struktur społecznych oraz dążenie do prywatyzacji i rekonstrukcji sfery publicznej. Skutkuje to rozpadem wielu tradycyjnych więzi i dezintegracją społeczności uznawanych przed nadejściem ery informacyjnej za trwałe, hierarchiczne i nierozerwalne.

Podobny sceptycyzm wyrażał Stanisław Lem, który twierdził, iż Internet nie tylko utrudnia kontakty między ludźmi, ale także prowadzi do dominacji języka angielskiego, naraża internautów na „wysyp informacji" oraz dostarcza bezmyślnej rozrywki (Bógdał-Brzezińska, Gawrycki, 2003: 53).

Rosnące uzależnienie od osiągnięć rewolucji informatycznej może wiązać się z poważnymi wyzwaniami dla poszanowania praw człowieka, przede wszystkim w kontekście nowych sposobów zbierania, archiwizacji i transferu danych, wraz z postępującym wyścigiem technologicznym informacje w formie cyfrowej mogą być bowiem coraz łatwiej zdobywane, nie tylko przez cyberprzestępców, ale także przez agencje rządowe (zob. Castro, 2010; Deibert, 2013; Fogelman, 1997: 181—189; Fajgielski, 2013: 143; Skwarzyński, 2013). Odwołując się m.in. do Orwellowskiej wizji wszechstronnie kontrolowanego społeczeństwa, wielu autorów często zwraca więc uwagę na zasadnicze

[53] Maurer, 2011, s. 17—18, 37—41; *Strategy for the period 2008—2011*, 2007; *Promotion of Activities*, 2011; *Cybersecurity: A global issue demanding a global approach*. Department of Economic and Social Affairs, United Nations, 12.12.2011: www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html; dostęp: 3.07.2013.

[54] Lu, Jen, Chang, Chou, 2006; *Cybercrime and Organized Crime*. United Nations Interregional Crime and Justice Research Institute: www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/organized_crime; dostęp: 3.07.2013.

[55] J. Robinson: *Is Social Networking Destroying Our Social Lives*? „Huffington Post", 1.02.2011: www.huffingtonpost.com/joe-robinson/social-network_b_816108.html; dostęp: 3.07.2013.

zagrożenia dla prawa do prywatności, które pojawiają się wraz z coraz szerszym wykorzystaniem komputerów i Internetu, zarówno w życiu prywatnym, jak i publicznym. Już w latach 90. XX wieku pisano w tym kontekście o ingerencji informacyjnej w życie prywatne czy centralizacji i zmonopolizowaniu informacji (Goban-Klas, Sienkiewicz, 1999: 67). Wyzwania te są szczególnie widoczne w przypadku działalności agencji rządowych. Oczywiście wykorzystanie nowoczesnych osiągnięć teleinformatyki z jednej strony prowadzi do podniesienia skuteczności działań służb bezpieczeństwa, z drugiej jednak umożliwia nadużycia związane z nieuprawnioną inwigilacją obywateli. O realności tego typu scenariusza świadczą kolejne skandale dotyczące monitorowania czy wręcz zbierania i przechowywania przez państwa szczegółowych informacji o użytkownikach sieci, które dotyczą nie tylko ich potencjalnie szkodliwej działalności, lecz także życia prywatnego. Na tym tle symboliczna stała się sprawa Edwarda Snowdena, który w 2013 roku ujawnił skalę aktywności wywiadowczej amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency — NSA) i Federalnego Biura Śledczego (Federal Bureau of Investigation — FBI) nie tylko wobec obywateli obcych państw, ale również wobec mieszkańców USA (program PRISM). Wydarzenie to miało trojakie konsekwencje: doprowadziło do wzmożenia międzynarodowej debaty poświęconej zagrożeniom wynikającym z rewolucji informatycznej[56], uświadomiło opinii publicznej zakres niejawnej współpracy między rządem Stanów Zjednoczonych a wielkimi korporacjami sektora IT, a ponadto doprowadziło do serii napięć w stosunkach międzynarodowych, co jednak nie stało się impulsem do wypracowania wiążących regulacji w tej materii[57].

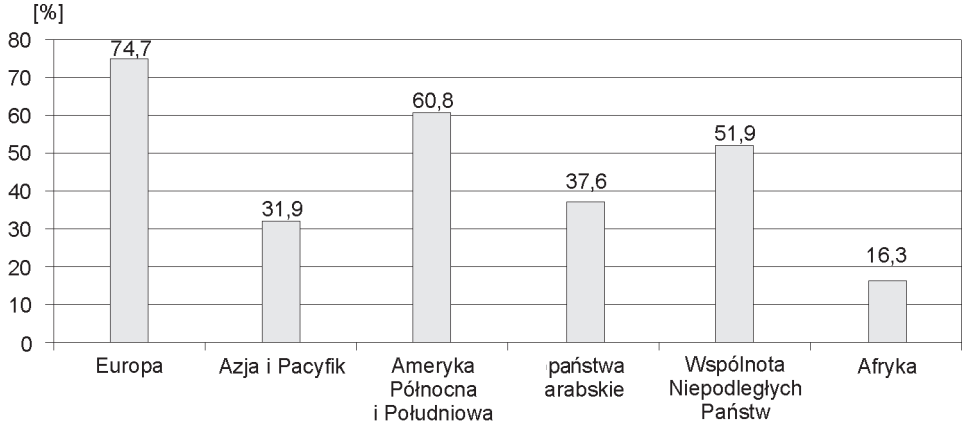
Wśród innych często wymienianych wyzwań mających związek z upowszechnieniem technologii teleinformatycznych wymienia się również:

- narastające problemy prawne, dotyczące interpretacji różnorodnych działań w sieci,

[56] Zob. Gellman, Poitras, 2013; G. Greenwald, L. Poitras, E. MacAskill: *Edward Snowden: US surveillance 'not something I'm willing to live under'*. „The Guardian" 8.06.2013: www.guardian.co.uk/world/2013/jul/08/edward-snowden-surveillance-excess-interview; dostęp: 17.07.2013; E. MacAskill: *Edward Snowden: NSA file source: 'If they want to get you, in time they will'*. „The Guardian" 10.06.2013: www.guardian.co.uk/world/2013/jun/09/nsa-whistleblower-edward-snowden-why; dostęp: 17.07.2013; G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, D. Rushe: *How Microsoft handed the NSA access to encrypted messages*. „The Guardian", 12.06.2013: www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data; dostęp: 17.07.2013.

[57] J. Watts: *Bolivian president's treatment stirs up fury in Latin America*. „The Guardian" 3.07.2013: www.guardian.co.uk/world/2013/jul/03/bolivian-president-morales-latin-america; dostęp: 17.07.2013; T. Paterson: *Germany prepares to charge UK and US intelligence over fresh bugging allegations*. „The Independent" 30.06.2013: www.independent.co.uk/news/world/europe/germany-prepares-to-charge-uk-and-us-intelligence-over-fresh-bugging-allegations-8680249.html.

- podział cyfrowy na społeczeństwa w mniejszym lub większym stopniu objęte procesami rewolucji informatycznej (zob. Wykres 5)[58],
- problemy społeczne związane z narastającymi różnicami w posiadanej przez użytkowników wiedzy, częściowym zanikiem kontaktów osobistych, tradycyjnych form komunikowania lub aktywności ruchowej,
- polaryzację dyskursu publicznego,
- „szum", „smog" informacyjny wynikający z mnogości źródeł pozyskiwania wiadomości lub ich złej jakości (szerzej: Achenbach, 1997),
- tendencje do centralizacji Internetu,
- wątpliwości natury etycznej związane m.in. z coraz większą dominacją różnorodnej rozrywki w sieci (Goban-Klas, Sienkiewicz, 1999: 96—122; Szpunar, 2012: 43).



Wykres 5. Liczba mieszkańców posiadających dostęp do Internetu w 2013 roku (w %)

Źródło: opracowanie własne na podstawie: *World Telecommunication/ICT Indicators Database*. International Telecommunication Union 2013.

Należy nadmienić, iż celowo pominięto najbardziej oczywiste i najistotniejsze z punktu widzenia omawianego tematu zagadnienie, jakim jest znaczenie rewolucji informatycznej dla bezpieczeństwa państw. Te kwestie szeroko omówiono w kolejnych rozdziałach. Mimo to już teraz warto podkreślić, iż postęp technologiczny wiąże się z wieloma fundamentalnymi zagrożeniami w tej dziedzinie. Jak bowiem zauważył Marek Madej, obecnie państwa nie posiadają takiej kontroli nad bezpieczeństwem jak w przeszłości. Jego zdaniem „możliwości nadzoru rządów nad przebiegiem życia społecznego oraz wszelkiego rodzaju wydarzeniami zachodzącymi na podległym ich władzy terytorium zmniejszają

[58] Jak zauważył Marek Pudełko (2013: 324—325), podział ten nakłada się na rozdźwięk między bogatą Północą a biednym Południem. W przypadku *digital divide* zwraca się jednak uwagę na wiedzę i umiejętności. Zob. także: Hundley, Anderson, Bikson, Neu, 2003: 55—131.

się wraz z upowszechnieniem się technologii informatycznych oraz coraz większą złożonością struktur powstałych z ich wykorzystaniem lub funkcjonujących w oparciu o nie" (Madej, 2009: 32—33). Analiza tych zagadnień jest tym istotniejsza, iż informacja — kluczowa dla rewolucji informatycznej — stała się zasobem strategicznym w systemie bezpieczeństwa państwa (zob. np. Bobrow, 2000), a wynikające z niej wiedza i technologie stały się podstawowym czynnikiem wytwórczym, co przekłada się m.in. na dochód narodowy, poziom rozwoju gospodarczego czy procesy decyzyjne w wymiarze ekonomicznym, politycznym lub społecznym. Zakłócenie działalności infrastruktury teleinformatycznej może zatem skutkować poważnymi konsekwencjami w niemal wszystkich obszarach funkcjonowania państwa (Liedel, 2011: 57). Należy również podkreślić, iż osiągnięcia w tej dziedzinie zostały szeroko zaadaptowane przez siły zbrojne, stworzyło to więc potencjalnie zupełnie nową arenę zmagań podczas konfliktu zbrojnego[59].

Mając na uwadze wszystkie powyższe rozważania, należy potwierdzić, iż rewolucja informatyczna, zgodnie z przewidywaniami Alvina Tofflera, rzeczywiście otworzyła w drugiej połowie XX wieku nowy etap rozwoju ludzkości. Bezprecedensowy rozwój naukowo-techniczny pozwolił raptem w ciągu kilku dekad dokonać fundamentalnej zmiany sposobu funkcjonowania nie tylko jednostek, ale także całych społeczeństw i państw, co przyniosło zarazem doniosłe korzyści, jak i poważne zagrożenia. Najważniejsze z perspektywy omawianego tematu jest jednak to, iż konsekwencją rewolucji informatycznej było wykształcenie nowej, „aterytorialnej" i niematerialnej sfery ludzkiej działalności, jaką jest cyberprzestrzeń. W ciągu kilkudziesięciu lat domena ta, której rdzeń stanowi Internet, stała się nie tylko obszarem swobodnej komunikacji, wymiany opinii, realizowania przedsięwzięć gospodarczych czy powstawania nowych więzi społecznych, lecz w XXI wieku stała się również źródłem wielu poważnych wyzwań dla bezpieczeństwa narodowego i międzynarodowego. Sytuacja ta udowodniła więc, iż utopijne wizje deterministów technologicznych, którzy skupiali się wyłącznie na pozytywnych cechach rewolucji informatycznej, dalece rozminęły się z rzeczywistością. Bez wątpienia nowe technologie zmieniły oblicze ludzkości, doprowadziły jednak również do pojawienia się wielowymiarowych patologii. Walka z nimi jest jednym z najpoważniejszych problemów całej społeczności międzynarodowej w XXI wieku.

[59] O skali tego zjawiska może świadczyć m.in. fakt, iż Edmund M. Glabus (2000: 81—82) porównał zastosowanie wojskowe wirusów biologicznych z wirusami komputerowymi oraz „kognitywnymi", właściwymi dla ery informacyjnej. Przez *wirus kognitywny* rozumiał on określoną informację, „mem", który wpływa na psychikę ludzką, rozprzestrzenia się i wpływa na określone wydarzenia. Zob. też Metz, 2000.

Rozdział 2

Cyberprzestrzeń jako źródło nowych wyzwań i zagrożeń dla bezpieczeństwa państw

2.1. Definicja cyberprzestrzeni

Jak wspomniano w poprzednim rozdziale, jednym z najdonioślejszych rezultatów rewolucji informatycznej było pojawienie się nowej sfery ludzkiej działalności, jaką jest cyberprzestrzeń. Wykształciła się ona dzięki powstaniu sieci komputerowych, jednak wbrew wielu potocznie formułowanym sądom nie jest ona tożsama z Internetem. Jest to obszar zdecydowanie szerszy, posiadający wyjątkowe cechy techniczne, które determinują jego rosnące znaczenie dla życia społecznego i politycznego. W związku z tym od lat toczy się ożywiona dyskusja na temat tego, czym w zasadzie jest ta kategoria. Warto szerzej się nad tym zastanowić, zrozumienie bowiem, czym jest cyberprzestrzeń, jakie są jej najistotniejsze cechy oraz jakie wynikają z tego wyzwania i zagrożenia dla bezpieczeństwa, jest warunkiem *sine qua non* realizacji postawionego we wstępie celu badawczego. Odpowiedź na pytanie, w jaki sposób państwa rywalizują i współpracują w cyberprzestrzeni, nie jest możliwa bez uchwycenia istoty środowiska tej aktywności.

Zdefiniowanie cyberprzestrzeni jest bez wątpienia kwestią niezwykle trudną, zarówno ze względu na jej skomplikowaną strukturę techniczną, jak i wynikające z tego konsekwencje społeczne. Bardzo trafnie kwestię tę ujął Ronald J. Deibert (2013: 10—11), który we wstępie do swojej książki *Black Code: Inside the Battle for Cyberspace* napisał:

> Rozejrzyj się wokół siebie. Czy widzisz kogoś, kto wpatruje się w swój smartfon? Ile razy sprawdziłeś dziś swój e-mail? Czy szukałeś kafejki z Wi-Fi, aby

> tego dokonać? Ilu ludziom wysłałeś dziś wiadomości tekstowe? […] Cyberprzestrzeń jest wszędzie. Pod koniec 2012 roku na świecie było więcej urządzeń mobilnych niż ludzi: telefonów komórkowych, laptopów, tabletów, konsol, a nawet podłączonych do Internetu samochodów. Niektórzy oceniają liczbę podłączonych do sieci urządzeń na 10 miliardów. Cyberprzestrzeń stała się tym, co badacze nazywają „całkowicie wciągającym środowiskiem", fenomenem, którego nie można uniknąć lub zignorować, coraz bardziej osadzonym w bogatych i biednych społeczeństwach, niedyskryminującą areną komunikacji. […] Cyberprzestrzeń jest obecnie nieuniknioną rzeczywistością, która owija naszą planetę złożoną skórą informacji i komunikacji. Kształtuje nasze działania i wybory, nieubłagalnie zbliżając nas do siebie. […] Współdzielona przestrzeń, globalna gmina, rozrośnięty plac publiczny.

Wydaje się, że słowa te obrazowo oddają, czym dziś stała się cyberprzestrzeń, łącząca w skali świata szeroką gamę podmiotów, od pojedynczych użytkowników aż po organizacje międzynarodowe, wchodzących ze sobą w interakcje w różnorodnych, wcześniej niewyobrażalnych płaszczyznach i konfiguracjach.

Mając na uwadze powyższe, próbę zdefiniowania *cyberprzestrzeni* warto jednak rozpocząć od etymologii tego pojęcia. Pierwotnie wywodzi się ono z literatury science fiction lat 80. XX wieku, skupiającej się wówczas w dużej mierze na przyszłych rezultatach rewolucji informatycznej. Wbrew potocznej opinii pojęcia tego nie ukuł wcale William Gibson, pojawiało się ono bowiem już w powieściach Vernora Vinge'ego (*True Names*) oraz Johna M. Forda (*Web of Angels*)[1]. To jednak właśnie Gibson przyczynił się do jego popularyzacji i zarazem do utworzenia nowego nurtu w literaturze tego czasu, który zaczął być określany mianem *cyberpunka*. Po raz pierwszy termin ten zastosował w opowiadaniu *Burning Chrome* z 1982 roku, a potem w słynnej powieści *Neuromancer* wydanej dwa lata później. *Cyberprzestrzeń* opisał tam następująco:

> Cyberprzestrzeń. Konsensualna halucynacja, doświadczana codziennie przez miliardy legalnych operatorów, w każdym narodzie, przez dzieci nauczane pojęć matematycznych… Graficzna reprezentacja danych pobranych z banków pamięci każdego komputera w systemie człowieka. Niewyobrażalna złożoność. Linie światła uszeregowane w nieprzestrzeni umysłu, klastry i konstelacje danych. Oddalone jak światła miasta (Gibson, 1984: 69).

Definicja to oczywiście literacka, traktująca cyberprzestrzeń jako swoistą halucynację, graficzne odwzorowanie danych, informacji w formie cyfrowej, w której ścierały się interesy wielkich koncernów. Bez względu na fakt, iż dość

[1] Zob. N. Gaiman: *Ten Years Ago*. NeilGaiman.com, 25.09.2006: http://journal.neilgaiman.com/2006/09/ten-years-ago.html; dostęp: 30.07.2013; Vinge, 2001.

odległa od rzeczywistości, w zasadniczym stopniu wpłynęła na upowszechnienie tego typu zagadnień w popkulturze. Dzięki zainspirowanym nią takim hollywoodzkim filmom, jak *Johny Mnemonic* czy *Matrix*, w społecznym wyobrażeniu cyberprzestrzeń zaczęła się kojarzyć obrazowo z niematerialną sferą, której manifestacją były zielone znaki spływające w dół ekranu komputera. W takim ujęciu cyberprzestrzeń opierająca się na dorobku rewolucji informatycznej miała więc z reguły określoną formę graficzną (Clarke, Knake, 2010: 69). Warto dodać, iż jej literackie rozwinięcie znalazło swój wyraz również w sławnej powieści Neila Stephensona z 1989 roku pod tytułem *Snow Crash* (Libicki, 2007: 5).

Koncepcja ta, jakkolwiek nienaukowa i głęboko osadzona w fikcji literackiej, została jednak zapożyczona dość szybko przez zachodnich naukowców, którzy dostrzegli jej przydatność do opisania nowej, niematerialnej sfery ludzkiej działalności, stworzonej przez komputery i ich sieci. Wykorzystanie terminu *cyberprzestrzeń* od lat spotyka się jednak z ostrą krytyką części badaczy, co wynika z faktu, iż nie jest to pojęcie *stricte* informatyczne i nie ma pierwotnego rodowodu naukowego. Kontrowersje budzi przede wszystkim przedrostek *cyber-*[2], który został zapożyczony przez autorów science fiction z cybernetyki, będącej nauką o systemach sterowania i przetwarzaniu informacji. W tym kontekście symboliczne wydają się rozważania przedstawiciela obszaru nauk technicznych Krzysztofa Lidermana (2012: 60—65), który stwierdził:

> w ostatnich latach można zauważyć coraz powszechniejsze używanie słów zaczynających się od przedrostka *cyber-*. […] Pojawia się on również w zbitkach słownych, takich jak *atak cybernetyczny* czy *obrona cybernetyczna*. […] Przyswajanych jest wiele takich słów wytrychów (najczęściej bezkrytycznie), bo uważa się powszechnie, że ich używanie świadczy o znajomości najnowszych światowych trendów.

Wymienił on szereg wątpliwości związanych m.in. z rozumieniem terminów z zakresu bezpieczeństwa teleinformatycznego. Jego zdaniem (Ibidem):

> stosowanie medialnej terminologii „cyberświata" do realnych działań i konstrukcji inżynierskich narusza ww. podstawowe zasady dobrej praktyki, ponieważ: coraz powszechniej używane terminy „cybercoś tam": nie mają jednoznacznych, powszechnie akceptowanych definicji; są nadmiarowe […], są niemierzalne; posługując się niezdefiniowanymi lub źle zdefiniowanymi terminami, nie można sformułować […] wymagań ani określić realnych celów; nie można budować […] skutecznych systemów np. zabezpieczających.

[2] Jak zauważyła Myriam Dunn-Cavelty (2008: 16), przedrostka *cyber-* przyjęło się używać powszechnie jako synonimu oznaczającego z grubsza 'z wykorzystaniem komputera' (*through the use of a computer*).

Autor zauważył ponadto, iż cyberprzestrzeń jako taka nie ma wiele wspólnego ze wspomnianą wcześniej nauką — cybernetyką (Ibidem). Opinia ta, podzielana przez niektórych przedstawicieli nauk technicznych, wydaje się właściwym przykładem, w oparciu o który można spróbować omówić, czym w zasadzie jest cyberprzestrzeń.

Przytoczone wyżej rozważania, jakkolwiek podniosły bardzo istotną i sygnalizowaną już kwestię poważnych problemów natury terminologicznej, są zarazem znamienne dla często odmiennej percepcji tych zagadnień z punktu widzenia nauk technicznych i nauk społecznych. Autor, krytykując wykorzystywane pojęcia, z braku lepszych propozycji rzeczywiście bazujące głównie na odpowiednikach amerykańskich, nie zauważył jednak, iż tę problematykę można postrzegać nie tylko z perspektywy czysto technicznych aspektów bezpieczeństwa sieci komputerowych. Służąc ludziom i będąc obszarem ich coraz bardziej złożonej działalności, stają się one przedmiotem badań nauk społecznych, w tym takich dyscyplin, jak nauki polityczne czy nauki o bezpieczeństwie. Te, bazując oczywiście na obiektywnych uwarunkowaniach technicznych, skupiają się jednak przede wszystkim na szeroko rozumianym aspekcie ludzkim. Do opisu występujących tu zjawisk nie wystarczą wyłącznie pojęcia proponowane przez nauki techniczne, szczególnie iż są one często zbyt wąskie, a co za tym idzie nie zawsze przydatne. Nie da się np. omówić politycznych, prawnych i militarnych konsekwencji ataków komputerowych organizowanych przez państwa, odnosząc się jedynie do ich cech w wymiarze technicznym. Jest to szczególnie widoczne w przypadku krytykowanego przez Krzysztofa Lidermana pojęcia *cyberprzestrzeni* (Ibidem, s. 62—63).

Mając to na uwadze, należy podkreślić, iż terminy naukowe częstokroć mają charakter umowny, luźno lub symbolicznie związany z rzeczywistym obiektem badań. Co ciekawe, nie jest tak jednak w przypadku omawianego pojęcia. Wbrew zaprezentowanym wyżej opiniom dość łatwo można odnaleźć zasadny związek między elementami cybernetyki a źródłosłowem pojęcia *cyberprzestrzeń*[3] (i kolejnych wywodzących się z niego nazw). Przede wszystkim warto zauważyć, iż w państwach zachodnich rozumienie cybernetyki jest do dziś zdecydowanie bardziej zróżnicowane niż w rodzimej literaturze specjalistycznej. W wielu definicjach tej nauki szczególnie mocno akcentowano nie sterowanie, lecz komunikowanie i przetwarzanie informacji. W efekcie tego na gruncie pewnych nurtów cybernetyki wyrosły technologie informatyczne, w tym np. badania nad sztuczną inteligencją (AI). Współcześnie niektóre jednostki naukowe zajmujące się cybernetyką prowadzą również badania m.in. nad robotyką. Warto ponadto zauważyć, że samo słowo *cybernetyka* jest kategorią bardzo pojemną. Jego nowoczesne rozumienie spopularyzowane przez Norberta Wienera samo w sobie rozmija się znacząco z jego historycznym rodowodem, przykładowo

[3] Pisali o tym m.in. Bogusław Pacek i Romuald Hoffmann (2013: 61).

Platon wykorzystywał je bowiem jako pojęcie oznaczające rząd, w 1845 roku francuski fizyk i matematyk André-Marie Ampère określił w ten sposób naukę o rządzie[4]. Na tej podstawie widać więc wyraźnie, iż *cybernetyka*, wywodząca się ze starogreckiego *kybernētēs* oznaczającego zarządcę, sternika, nawigatora, bez względu na głosy sceptyków ma jednak wyraźny związek z kategorią pojęć wyrosłych na gruncie „cyberprzestrzeni". Stosunkowo łatwo można odnaleźć analogię, która mogła posłużyć zachodnim autorom za podstawę przyjęcia konwencji terminologicznej opartej o przedrostek *cyber-*. Wszakże, jak wspomniano w poprzednim rozdziale, istotą rewolucji informatycznej i wszystkich procesów technologicznych w jej ramach była zmiana charakteru informacji oraz sposobów jej przetwarzania czy archiwizowania. To właśnie na informacji w formie cyfrowej są oparte systemy i sieci komputerowe, te zaś są podstawowymi elementami składowymi cyberprzestrzeni. Tymczasem komunikowanie i informacja są również podstawowymi kategoriami cybernetyki.

Na tej podstawie można więc odnieść się szerzej do głównego zarzutu dotyczącego samego pojęcia *cyberprzestrzeni*, a następnie spróbować je zdefiniować. Przede wszystkim należy zgodzić się ze stwierdzeniem, iż pierwsze przytoczone wyżej próby scharakteryzowania tej sfery miały charakter nienaukowy, a przez to były nieprzydatne z punktu widzenia procesu badawczego. Jednak już w latach 90. XX wieku zaczęło powstawać wiele mniej lub bardziej trafnych definicji naukowych tego pojęcia, które starały się uchwycić istotę nowej domeny, wykształconej dzięki rewolucji informatycznej. Jakkolwiek częstokroć bardzo się one od siebie różniły, posiadały jedną cechę wspólną. Wbrew krytyce niektórych przedstawicieli nauk technicznych *cyberprzestrzeń* była i jest ujmowana jako pewna kategoria zbiorcza, charakteryzująca domenę funkcjonującą w oparciu o wcześniej jasno zdefiniowane elementy infrastruktury (tele)informatycznej, w tym m.in. komputery, składające się z nich sieci, oprogramowanie itp. Definicja taka została ukuta przede wszystkim z dwóch powodów. Po pierwsze: aby nie wymieniać całej gamy urządzeń i aplikacji za każdym razem, gdy omawiane procesy rozciągają się na wiele różnych aspektów ICT, drugim powodem

[4] Aby uświadomić sobie szeroki zakres form cybernetyki oraz jej różnorodne rozumienie, można przytoczyć kilka jej definicji. Chris Lucas, opierając się na ujęciu Norberta Wienera, scharakteryzował ją jako „naukę efektywnej organizacji, kontroli i komunikacji w zwierzętach i maszynach. To sztuka sterowania, regulacji i stabilności". Według Charlesa A. Finka cybernetyka jest nauką traktującą o „niewidzialnych procesach, które pobudzają dynamiczne jednostki". Peter Corning uznał ją za naukę interesującą się celowością, przepływami informacji czy procesem podejmowania decyzji „na wszystkich poziomach żywych systemów". Gregory Bateson uznał ją za gałąź matematyki zajmującą się problemami kontroli, powtarzalności i informacji. Zob. Mazur, 1999; Katz, Smith-Macklin, 2007; *Cybernetics — a Definition*. Pangaro: www.pangaro.com/published/cyber-macmillan.html; dostęp: 6.03.2013; *Symposium: Theories and Metaphors of Cyberspace*. 09—12.04.1996, University of Vienna: http://pespmc1.vub.ac.be/CYBSPASY.html; dostęp: 6.03.2013; *Defining cybernetics*: www.asc-cybernetics.org/foundations/definitions.htm; dostęp: 6.03.2013.

była natomiast świadomość, iż w wyniku rewolucji technologicznej wykształciła się wyjątkowa, niematerialna i „aterytorialna" sfera działalności człowieka[5]. Z perspektywy nauk społecznych wykorzystanie tego typu zbiorczego terminu, jakim jest *cyberprzestrzeń*, wydaje się więc jak najbardziej uzasadnione — wszak jej właściwości zyskały zasadnicze znaczenie zarówno dla funkcjonowania jednostek, ich zbiorowości, jak i całych wręcz społeczeństw i państw.

Na tej podstawie warto podjąć próbę zrozumienia, czym *de facto* jest cyberprzestrzeń i co się na nią składa. Jak wspomniano, nie ma zgody badaczy co do jednoznacznego rozumienia tego terminu. Istnieje szeroki konsensus co do pewnych wskazanych wyżej ogólników, szczegółowe jej zdefiniowanie rodzi już jednak spore kontrowersje. Od trzech dekad próby takie podejmują różnorodne grupy, przedstawiciele nauk technicznych, ścisłych, społecznych, politycy, eksperci pracujący dla instytucji i służb państwowych czy wreszcie organizacje międzynarodowe. Warto przytoczyć szereg najbardziej popularnych definicji naukowych, które mogą być przydatne do zrozumienia tego zagadnienia. W dużym uproszczeniu można je pogrupować w dwie kategorie: definicje ogólne i posługujące się pojęciami abstrakcyjnymi oraz interpretacje zdecydowanie bardziej kompleksowe, rozbudowane, wymieniające poszczególne elementy składowe tej domeny.

Rozpoczynając charakterystykę od definicji abstrakcyjnych i ogólnych, można przywołać klasyczny sposób ujmowania tego pojęcia w encyklopediach na przykładzie *The American Heritage Science Dictionary* (2002) w którym stwierdzono, iż *cyberprzestrzeń* jest „medium elektronicznym [złożonym — M.L.] z sieci komputerowych, w którym ma miejsce komunikacja online". Jedną z pierwszych ciekawszych definicji tego typu w literaturze naukowej zaproponowali w 1996 roku Roger C. Molander, Andrew S. Riddile i Peter A. Wilson (1996: iii), którzy przestrzeń teleinformatyczną utożsamiali z „globalną infrastrukturą informacyjną". W kolejnych latach pojawiło się zdecydowanie więcej podobnych, mało sprecyzowanych interpretacji tego terminu. Pierre Delvy uznał np. *cyberprzestrzeń* za „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie". W jego rozumieniu cyberprzestrzeń obejmowała więc wszystkie środki komunikacji elektronicznej[6]. Marie Laure Ryan błędnie stwierdziła, iż *cyberprzestrzeń* stanowi wygenerowaną przez komputer rzeczywistość wirtualną[7]. Steven A. Hildreth (2002) uznał ją za „wzajemną łączność między ludźmi za pomocą komputerów i telekomunikacji, bez względu na geo-

[5] W anglojęzycznej literaturze specjalistycznej z zakresu nauk technicznych termin *cyberprzestrzeń* jest wykorzystywany powszechnie. Zob. np. Madnick, Choucri, Camiña, Woon, 2012.

[6] *Cyberprzestrzeń — definicje*. Techsty — Literatura i Nowe Media: www.techsty.art.pl; dostęp: 21.09.2013.

[7] Ibidem.

grafię". Można wspomnieć również o Tomaszu Szubrychcie (2005: 173), który zaproponował następującą definicję: „przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Ułatwia ona użytkownikowi sieci kontakty w czasie rzeczywistym. Obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych". Diane Saco (2002: 100, cyt. za: Rothert, 2004: 45) zauważyła z kolei, iż jest ona „kulminacją osiągnięć technologii: komputeryzacji elektronicznej (pokawałkowana przestrzeń mikstury elektronowo-atomowej), sieci komputerowych (zróżnicowana przestrzeń sieciowa łącząca *tu* i *tam*) i wreszcie komputerów osobistych (otwarta przestrzeń mieszających się ze sobą zinstytucjonalizowanych i indywidualnych praktyk online)". W 2006 roku Michael Wynn użył natomiast pewnej przenośni, podkreślając, iż *cyberprzestrzeń* to „domena, w której [amerykańskie — M.L.] Siły Powietrzne latają i walczą" (Rid, 2012: 5—32). Z perspektywy nauk ekonomicznych nazbyt abstrakcyjne podejście zaproponowała Joanna Smith-Bers. Jej zdaniem *cyberprzestrzeń* jest to „elektroniczna granica, za którą banki mogą operować w sposób bardziej opłacalny, oferować produkty i usługi praktycznie nieograniczonej liczbie bazie klientów" (Smith-Bers, 1997: 107).

W literaturze specjalistycznej można jednak odnaleźć wiele zdecydowanie bardziej kompleksowych definicji tego pojęcia. Daniel T. Kuehl (2009, cyt. za: Schreier, 2015: 11) uznał np. *cyberprzestrzeń* za „domenę operacyjną", której unikalną cechą jest wykorzystanie „elektroniki i spektrum elektromagnetycznego do tworzenia, przechowywania, modyfikacji, wymiany i wyzyskiwania informacji poprzez wzajemnie powiązane systemy oparte na technologiach informacyjnych i komunikacyjnych oraz powiązaną z nimi infrastrukturę". Według Thomasa C. Wingfielda (2000: 17) nie jest to miejsce w fizycznym, materialnym rozumieniu, nie podlega bowiem żadnym próbom pomiarów fizycznych czy kontinuum czasoprzestrzennemu. Jego zdaniem jest to więc „skrótowe określenie, które dotyczy środowiska stworzonego zarówno przez kooperatywne sieci komputerów, systemów jak i infrastrukturę telekomunikacyjną". Pierwsza część definicji wydaje się jednak nie do końca właściwa, jak bowiem zauważyły Kristin M. Finklea i Catherine A. Theohary (2013: 1—3) w raporcie Congressional Research Service, w cyberprzestrzeni granice fizyczne co prawda nie obowiązują, jest ona jednak ściśle związana ze światem materialnym dzięki podtrzymującej ją infrastrukturze teleinformatycznej. Podobne stanowisko zajął Nils Melzer (2011: 4), który uznał *cyberprzestrzeń* za „globalnie połączoną sieć cyfrowej infrastruktury informacyjnej i komunikacyjnej, obejmującą Internet, sieci telekomunikacyjne, systemy komputerowe oraz zawierające się w nich dane". W ten sam sposób rozumowali Richard A. Clarke i Robert K. Knake (2010: 69—70). W zaproponowanej przez nich definicji przestrzeń teleinformatyczna objęła zarówno komputery, składające się na nie komponenty (np. procesory), jak ich sieci (w tym łączące je kable). Ich zdaniem „cyberprzestrzeń to wszystkie sieci

komputerowe na świecie i wszystko, z czym się łączą i co kontrolują". W rozwiniętej formie ujęcie to zaprezentował również Fred Schreier (2015: 10—11). Udało mu się z jednej strony uniknąć pewnych wad przytoczonych wyżej prób, z drugiej natomiast zebrać w całość ich najbardziej wartościowe elementy. Jak stwierdził:

> cyberprzestrzeń, nowy, piąty teatr wojny, po lądzie, wodzie, powietrzu i kosmosie, jest [złożony — M.L.] ze wszystkich sieci komputerowych na świecie oraz wszystkiego, co łączą i kontrolują poprzez kable, światłowody czy bezprzewodowo. To nie tylko Internet — otwarta sieć sieci […]. Cyberprzestrzeń obejmuje więc Internet plus wiele innych sieci komputerowych, włącznie z tymi, które nie powinny być dostępne z Internetu. Część z tych prywatnych sieci wygląda jak Internet, są one jednak, przynajmniej teoretycznie, odrębne. Innymi częściami cyberprzestrzeni są sieci transakcyjne, które zajmują się takimi rzeczami, jak przesył danych o przepływach pieniężnych, handlu akcjami giełdowymi i transakcjach kart kredytowych. Dodatkowo istnieją sieci, które są systemami SCADA (Supervisory Control and Data Acquisition) pozwalającymi maszynom komunikować się ze sobą […]. Tak więc cyberprzestrzeń składa się z istniejących obecnie dwóch miliardów komputerów, plus serwery, routery, przełączniki, światłowody i kable oraz komunikacja bezprzewodowa, które pozwalają na funkcjonowanie infrastrukturze krytycznej.

Autor dodał także, iż środowisko teleinformatyczne istnieje w dwóch wymiarach: materialnym i niematerialnym, jednocześnie przekracza więc granice geograficzne i zawiera się w nich. Warto jednak zauważyć, iż nie wszyscy autorzy podzielają takie stanowisko (zob. np. Hare, 2009).

Interesujące i kompleksowe próby scharakteryzowania *cyberprzestrzeni* można odnaleźć również na gruncie polskiej literatury specjalistycznej. Ernest Lichocki (2008: 8) stwierdził na przykład:

> cyberprzestrzeń staje się w XXI wieku „układem nerwowym" państwa. Jest to system sterowania krajem, złożony z tysięcy połączonych ze sobą systemów teleinformatycznych, które pozwalają działać państwowym podsektorom infrastruktury. Cyberprzestrzeń z Internetem stworzyła istotne zależności, które w nieprzewidywalny i groźny sposób zmieniają swoją naturę. Systemy teleinformatyczne, a szczególnie oprogramowanie zawarte w nich, mają wiele słabych punktów, które mogą umożliwić przeprowadzenie cyberataku.

Marek Madej (2009: 28) za Agnieszką Bógdał-Brzezińską i Marcinem Florianem Gawryckim uznał natomiast *cyberprzestrzeń* za „ogół powiązań o charakterze wirtualnym („nieprzestrzennym" w sensie fizycznym, niematerialnym i ageograficznym) powstałych i funkcjonujących dzięki technologiom informatycznym oraz ich fizycznym manifestacjom (komputery, infrastruktura telekomu-

nikacyjna)". W ciekawy sposób ujęła tę kwestię Agnieszka Rothert (2004: 45). Jej zdaniem mamy w tej dziedzinie do czynienia z

> potężną dawką niejasności i paradoksów. „Sieciowość" obejmuje oprócz ludzi i komputerów także działanie polegające na przesyłaniu danych poprzez sieć, co więcej są to różne systemy sieciowe […] protokoły, zasady dostępu oraz rozmaite sposoby komunikacji komputerowej. Przy czym „sieciowość" ma też szersze znaczenie — staje się modelem analizy w wielu naukach, w tym także społecznych. Cyberprzestrzeń istnieje też w wymiarze społecznym przejawiającym się nie tylko w praktykach online, ale w różnych koncepcjach, czym jest ta przestrzeń i jakie są jej sens lub przesłanie.

Osobno należy omówić zasygnalizowane wcześniej definicje nienaukowe, które pojawiają się w ostatnich latach w dokumentach i strategiach zarówno państw, jak i organizacji międzynarodowych. Wydaje się, iż najwięcej tego typu prób poczyniły służby i instytucje Stanów Zjednoczonych. W 2001 roku amerykański Departament Obrony uznał *cyberprzestrzeń* za „globalną domenę zawierającą się w środowisku informacyjnym, składającą się ze współzależnych sieci infrastruktur teleinformatycznych, obejmujących Internet, sieci telekomunikacyjne, systemy komputerowe i […] procesory oraz kontrolery" (*Department of Defense Dictionary*, 2001: 41). W *The National Military Strategy for Cyberspace Operations* z 2006 roku zdefiniowano ją jako „domenę charakteryzującą się wykorzystaniem elektroniki i spektrum elektromagnetycznego do przechowywania, modyfikowania i wymiany danych poprzez usieciowione systemy i towarzyszącą im fizyczną infrastrukturę" (s. 9). W *Department of Defense Strategy for Operating in Cyberspace* z lipca 2011 roku (s. 1) stwierdzono natomiast:

> Cyberprzestrzeń jest właściwością definiującą nowoczesne życie. Jednostki i zbiorowości na całym świecie łączą się, nawiązują kontakty i organizują się w cyberprzestrzeni i przez cyberprzestrzeń. […] cyberprzestrzeń będzie coraz bardziej wpleciona w tkankę życia codziennego na całym świecie. […] jest kluczowym sektorem globalnej gospodarki. Cyberprzestrzeń stała się inkubatorem nowych form przedsiębiorczości, rozwoju technologii, rozprzestrzeniania wolności słowa i nowych sieci społecznych, które napędzają naszą gospodarkę i stanowią odbicie naszych wartości.

W *Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations* z kwietnia 2011 roku uznano ją za „medium elektroniczne, poprzez które informacja jest tworzona, transmitowana, odbierana, przechowywana, przetwarzana i kasowana" (s. 20).

W niemieckiej strategii cyberbezpieczeństwa (*Cyber Security Strategy for Germany*) z lutego 2011 roku przyjęto natomiast zdecydowanie węższe rozumienie tego terminu. Stwierdzono, iż jest to

> przestrzeń wirtualna złożona ze wszystkich systemów IT na poziomie danych, w skali globalnej. Fundamentem cyberprzestrzeni jest Internet, jako uniwersalna i ogólnodostępna […] sieć, która może być uzupełniona i rozbudowana przez jakąkolwiek liczbę innych, dodatkowych sieci danych. Systemy IT w izolowanej przestrzeni wirtualnej nie są częścią cyberprzestrzeni (s. 14).

Z kolei we francuskiej *Défense et securité des systèmes d'information. Stratégie de la France* (s. 3, 21) przestrzeń teleinformatyczną uznano za „przestrzeń komunikacyjną stworzoną przez światowe połączenie zautomatyzowanych, cyfrowych urządzeń przetwarzających dane". Ciekawą interpretację tej domeny zawarto również we wstępie, napisanym przez Francisa Delona, sekretarza generalnego ds. obrony i bezpieczeństwa narodowego V Republiki. Stwierdził on, iż cyberprzestrzeń stała się swoistym wirtualnym polem bitwy, miejscem konfrontacji różnorodnych grup działających dla zbierania prywatnych danych, szpiegostwa przemysłowego, zakłócania usług zapewniających działanie gospodarki czy tworzenia zagrożeń dla narodowej suwerenności. Z drugiej strony zauważył jednak, iż stanowi ona w pewnym sensie „wieżę Babel", będąc miejscem spotkania kultur, wartości, idei czy informacji w czasie rzeczywistym. Ciekawe ujęcie zawarto również w strategii cyberbezpieczeństwa Kanady (*Canada's Cyber Security Strategy*, 2010: 2). Według niej *cyberprzestrzeń* jest swoistym „elektronicznym światem, stworzonym przez połączone ze sobą sieci IT oraz informacje w nich zawarte". Stanowi swoistą globalną wioskę, „gminę" łączącą użytkowników w celu „wymiany idei, usług i przyjaźni". Widać więc wyraźnie, iż zrezygnowano tu z poważniejszej próby scharakteryzowania jej technicznych właściwości na rzecz pewnego wyidealizowanego spojrzenia na jej rolę społeczną.

Próby zdefiniowania *cyberprzestrzeni* były i są podejmowane także przez polskich decydentów. Przykładowo według projektu *Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011—2016* (2010: 6) jest to „cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Jak zauważył Radosław Bania (2012: 185—186), definicja ta posiada kilka istotnych cech. Jego zdaniem

> eksponuje istotną rolę przekazu informacyjnego. Informacja musi być jednak zawsze traktowana, dwojako — po pierwsze jako przekaz zawierający treści, które da się przesłać od jednej osoby do drugiej, a po drugie jako medium, za pomocą którego ten przekaz się dokonuje. W przypadku cyberprzestrzeni mamy do czynienia z taką sytuacją. Z jednej strony zawarte są w niej pewne treści, które w dalszej kolejności krążą pomiędzy nadawcami i odbiorcami. Zmiana jakościowa, jaka w danym przypadku dotyczy przekazu informacyjnego, przede wszystkim polega na istnieniu bez mała nieograniczonej, limito-

> wanej jedynie pojemnością wszystkich spiętych w sieci dysków twardych oraz na szybkości, z jaką transfer się dokonuje.

Definicja ta została później rozszerzona w *Polityce Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej* z marca 2013 roku. Stwierdzono w niej, iż jest to:

> przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z art. 2 ust. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz.U. nr 156, poz. 1301, z późn. zm.), art. 2 ust. 1a *Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (Dz.U. nr 113, poz. 985, z późn. zm.) oraz art. 3 ust. 1 pkt 4 *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej* (Dz.U. nr 62, poz. 558, z późn. zm.)[8].

Mniej lub bardziej spójne definicje *cyberprzestrzeni* pojawiają się również od lat w wyniku prac prowadzonych przez organizacje międzynarodowe. Catherine Ashton, wysoka przedstawiciel ds. zagranicznych i polityki bezpieczeństwa Unii Europejskiej, podczas konferencji poświęconej bezpieczeństwu teleinformatycznemu w Budapeszcie w październiku 2012 roku podkreśliła bardzo szerokie spektrum dziedzin życia obejmowanych przez tę domenę: „wszystkie kluczowe usługi w naszych społeczeństwach zależą od cyberprzestrzeni — polegamy na niej, jeśli chodzi o transport, zaopatrzenie w prąd i wodę dla naszych domów, komunikację, łączność". Zaznaczyła przy tym, iż wynikająca z tego słabość może „przyciągnąć niszczycielskie siły" (Ashton, 2012b: 2). Zdecydowanie węższe rozumienie tego pojęcia przyjęto natomiast w *Cybersecurity Strategy of the European Union* z lutego 2013 roku. Co prawda nie zdefiniowano go jednoznacznie, jednak w tekście dokumentu w wielu miejscach utożsamiano go głównie z siecią Internet. O wiele bardziej zaawansowane prace w tej materii prowadzone są od lat przez Sojusz Północnoatlantycki. W bardzo ciekawy sposób ujęto to zagadnienie w jednej z najgłośniejszych publikacji eksperckich NATO poświęconych bezpieczeństwu teleinformatycznemu. W *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, ed., 2013: 211)

[8] *Polityka Ochrony*, 2013, s. 6. Zob. także: *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*. Dz.U. z 2005 r., nr 64, poz. 565; Dz.U. z 2006 r., nr 12, poz. 65, nr 73, poz. 501; Dz.U. z 2008 r., nr 127, poz. 817; Dz.U. z 2009 r., nr 157, poz. 1241; Dz.U. z 2010 r., nr 40, poz. 230, nr 167, poz. 1131, nr 182, poz. 1228; Dz.U. z 2011 r., nr 112, poz. 654, nr 185, poz. 1092, nr 204, poz. 1195; Dz.U. z 2012 r., poz. 1407.

stwierdzono, iż cyberprzestrzeń jest „środowiskiem uformowanym przez komponenty fizyczne i niefizyczne, charakteryzujące się wykorzystaniem komputerów i spektrum elektromagnetycznego do przechowywania, modyfikowania oraz wymiany danych przy wykorzystaniu sieci komputerowych". Bardzo ciekawą definicję zaproponował również Międzynarodowy Związek Telekomunikacyjny. W *ITU Toolkit for Cybercrime Legislation* (2010: 12) uznano ją za „fizyczny i niefizyczny obszar stworzony i/lub złożony z części lub całości następujących elementów: komputerów, systemów komputerowych, sieci, ich programów komputerowych, danych komputerowych, treści danych, ich przepływu oraz samych użytkowników".

Jak więc widać wyraźnie, w ciągu ostatnich dwóch dekad opracowano wiele bardzo zróżnicowanych definicji *cyberprzestrzeni*. Niektóre skupiają się głównie na bardziej ogólnych, często abstrakcyjnie ujmowanych zasadach jej funkcjonowania. Inne starają się podejść do zagadnienia bardziej kompleksowo, ujmując zarówno wątki techniczne, jak i społeczne. Należy przy tym zauważyć, iż nie ma zgody badaczy nawet co do spraw — wydawałoby się — tak obiektywnych, jak jej właściwości techniczne. Część z nich wskazywała, iż cyberprzestrzeń ma charakter wyłącznie niematerialny lub nie obejmuje komputerów nie podłączonych do sieci. Na tym tle wydaje się, iż trafną definicję zaproponował Alexander Melnitzky (2012: 557). Jego zdaniem z jednej strony cyberprzestrzeń stała się swoistym „globalnym kanałem" informacji, który przekracza fizyczne ograniczenia, z drugiej strony według autora na cyberprzestrzeń składają się również miedziane kable, światłowody, wieże przekaźnikowe, transpondery satelitarne czy routery internetowe. W takim rozumieniu cyberprzestrzeń, przekraczając przestrzeń fizyczną, jest w niej jednak bezpośrednio osadzona dzięki infrastrukturze teleinformatycznej. Podobne podejście zaprezentował Martin C. Libicki, który podzielił cyberprzestrzeń na trzy płaszczyzny: fizyczną (kable, routery itp.), syntaktyczną (format informacji w cyberprzestrzeni oraz sposoby instrukcji i kontroli systemów teleinformatycznych) oraz semantyczną (informacje zrozumiałe dla ludzi). Jak zaznaczył, uzyskanie dostępu do jednej z tych płaszczyzn czy też „podbicie" jej nie oznacza bynajmniej kontroli nad innymi, np. opanowanie fizycznej infrastruktury teleinformatycznej (płaszczyzny fizycznej) nie musi wiązać się z uzyskaniem dostępu do warstwy syntaktycznej, kontrolowanie warstwy syntaktycznej nie musi z kolei polegać na równoległym dostępie do płaszczyzny semantycznej. Libicki wyróżnił ponadto kilka interesujących cech charakterystycznych tej domeny. Według niego:

1. Cyberprzestrzeń została stworzona przez człowieka.
2. Jest ona konstruktem replikowalnym, a więc istniejącym w wielu miejscach naraz i możliwym do naprawy.
3. Cyberprzestrzeń może istnieć w wielu formach i manifestacjach.
4. Prawa rządzące cyberprzestrzenią nie muszą być zawsze zgodne z prawami fizyki czy tymi ustanawianymi przez człowieka.

5. Niektóre aspekty cyberprzestrzeni na ogół mają trwały charakter. Zaliczył on do nich m.in. reguły nią rządzące, w tym te, które oparte są na matematyce (prawa kryptografii) lub zasady określane przez twórców oprogramowania (Libicki, 2007: 4—9).

Tak kompleksowe ujęcia cyberprzestrzeni wydają się jak najbardziej słuszne, dają bowiem szerokie pole do dalszej analizy. Czym więc ona jest w praktyce? Stanowi domenę przetwarzania, przechowywania i przesyłania informacji w formie cyfrowej, funkcjonującą w oparciu o transmisję sygnałów cyfrowych oraz promieniowanie elektromagnetyczne. Jest przestrzenią w swojej istocie niematerialną, ale funkcjonującą dzięki infrastrukturze teleinformatycznej, która te sygnały wytwarza i przesyła. Aby zrozumieć tę zależność, można przytoczyć najprostszy przykład. Podejmując próbę wejścia na jakąkolwiek stronę WWW, użytkownik komputera korzysta z reguły z klawiatury i myszy, dzięki którym wydaje komputerowi określone polecenia (włączenie przeglądarki internetowej, wpisanie adresu, komenda Enter). Naciskając klawisz bądź manipulując myszą, dokonuje się działalności *stricte* fizycznej, która powoduje jednak rozpoczęcie operacji arytmetycznych i logicznych w komputerze oraz transmisję sygnałów. Tak więc użytkownik, oddziałując na interfejs urządzenia informatycznego, osiąga efekt z gruntu niematerialny. Tym samym podejmując działania w świecie materialnym, w oparciu o mierzalną i geograficznie zlokalizowaną infrastrukturę, wchodzi w „aterytorialny" świat cyberprzestrzeni. Można się więc zgodzić ze słowami Agnieszki Bógdał-Brzezińskiej i Marcina Floriana Gawryckiego (2003: 37), którzy stwierdzili, iż „obszar ten, widziany przez pryzmat techniki, cechują inne jakości aniżeli tradycyjną przestrzeń geograficzną".

W takim rozumieniu domena ta istnieje i funkcjonuje niejako wewnątrz i poprzez infrastrukturę teleinformatyczną, jest nią więc każdy bit danych przechowywanych, przetwarzanych i przesyłanych w komputerach oraz sieciach komputerowych, a także wszystkich innych elementach składających się na szeroko pojętą infrastrukturę teleinformatyczną. Na tym tle należy podkreślić, iż podstawowym elementem cyberprzestrzeni są naturalnie komputery, choć istnieją rozbieżne opinie, czy wszystkie, czy też jedynie te, które są podłączone do Internetu. Wbrew temu, co stwierdzono w niemieckiej strategii cyberbezpieczeństwa, trudno sobie wyobrazić analizę przestrzeni teleinformatycznej czy też działania na rzecz jej ochrony, nie biorąc pod uwagi komputerów offline. Warto w tym kontekście zwrócić uwagę na trzy kwestie. Przede wszystkim mimo braku połączenia z siecią komputery nadal mogą pełnić istotne funkcje z perspektywy interesu jednostek, przedsiębiorstw czy też całych społeczeństw i państw: kontrolują maszyny, pomagają w obliczeniach, wspomagają edukację i rozwój, zachowują zatem istotny wpływ na funkcjonowanie różnych dziedzin życia człowieka. Ponadto wbrew pozorom komputery, które nie są podłączone do sieci, posiadają możliwości komunikowania z innymi urządzeniami bądź

ich sieciami, potencjalnie każdy z nich może mieć kontakt z resztą cyberprzestrzeni mimo tego, że stanowi z jej perspektywy ośrodek izolowany. Służą temu różnorodne nośniki danych, takie jak CD-R, DVD czy pamięci USB, które są wykorzystywane na co dzień przez miliony użytkowników. Jest to szczególnie istotne z perspektywy bezpieczeństwa teleinformatycznego, wielokrotnie dochodziło bowiem do sytuacji, w której teoretycznie bezpieczne dane znajdujące się na komputerze niemającym dostępu do Internetu, były wykradane dzięki wykorzystaniu możliwości oferowanych przez niektóre typy złośliwego oprogramowania. W dobie rozwoju sieci bezprzewodowych i urządzeń mobilnych bardzo często występuje również sytuacja, w której użytkownik jedynie przez pewien czas korzysta z Internetu, następnie zaś go opuszcza. Z perspektywy metodologicznej poważnym błędem byłoby zatem ignorowanie procesów i wydarzeń, które zachodzą w komputerach odciętych od Internetu, przyjmując tak zawężoną optykę badawczą, należałoby bowiem pominąć np. chińskie włamania do baz danych amerykańskiej armii, które z zasady dostępu do Internetu nie posiadają.

Kontynuując te rozważania, oprócz tradycyjnie rozumianych komputerów stacjonarnych lub ich wersji przenośnych do cyberprzestrzeni można zaliczyć wiele innych urządzeń elektronicznych, które mogą zostać w jakikolwiek sposób zaprogramowane. Są nimi np. smartfony, czytniki *e-booków* lub konsole do gier. Można wymienić jednak urządzenia, które są już mniej oczywiste: bardziej zaawansowane telewizory (posiadające pamięć bądź łącze sieciowe) czy nawet nowsze samochody. *Sensu largo* wszystkie są albo komputerami, albo też zawierają w swojej architekturze programowalne elementy (np. komputer pokładowy w samochodzie). Słuszność takiego podejścia udowodniło doświadczenie przeprowadzone w lipcu 2013 roku. Wykazało ono, iż hakerzy są obecnie zdolni złamać zabezpieczenia systemów kontrolujących funkcjonowanie najbardziej zaawansowanych technologicznie pojazdów, przejmując np. kontrolę nad kierownicą[9]. Na tym tle rdzeniem cyberprzestrzeni jest oczywiście wspólna platforma komunikacyjna, jaką jest Internet. Jak wspomniano jednak wyżej, również pojedyncze komputery oraz wyizolowane sieci zaliczają się do tej kategorii. Na koniec należy stwierdzić, iż cyberprzestrzeń osadzona jest w ogromnej liczbie innych elementów składających się na infrastrukturę teleinformatyczną umożliwiającą archiwizację, przetwarzanie oraz transfer danych w formie cyfrowej. Mogą to być mające fundamentalne znaczenie routery, stacje przekaźnikowe (w przypadku wysyłających fale elektromagnetyczne sieci bezprzewodowych) czy zwykłe miedziane kable oraz światłowody.

[9] *Printers: The New Hackers' Instrument of Havoc*. DeviceLine Blog, 26.01.2011: https://mocana.com/blog/tag/cyber-attacks; dostęp: 6.03.2013; *Hakerzy opanowali samochody. Chcieli udowodnić, że mogą*. TVN 24, 28.07.2013: www.tvn24.pl/internet-hi-tech-media,40/hakerzy-opanowali-samochody-chcieli-udowodnic-ze-moga,342943.html; dostęp: 1.08.2013.

2.2. Właściwości techniczne cyberprzestrzeni

Przyjmując powyższe rozumienie cyberprzestrzeni, warto bliżej scharakteryzować jej najważniejsze właściwości techniczne, istotne z perspektywy pojawiających się zagrożeń dla bezpieczeństwa państw. Wydaje się, iż należałoby ten wątek rozpocząć od omówienia głównych wskazanych wyżej elementów, na których cyberprzestrzeń jest osadzona. Podstawowym urządzeniem tworzącym przestrzeń teleinformatyczną jest bez wątpienia komputer. Mając na uwadze rozważania z rozdziału pierwszego, można zdefiniować *komputer* jako „urządzenie elektroniczne, zdolne do (1) przyjmowania, przechowywania i logicznego manipulowania tekstem lub danymi, które zostały wprowadzone, (2) ich przetwarzania i wytworzenia […] rezultatów bądź decyzji, na bazie instrukcji zawartych w programach”[10]. Według innego podejścia jest to „elektroniczna maszyna cyfrowa, stosowana do przetwarzania, gromadzenia i wyszukiwania informacji za pomocą odpowiedniego oprogramowania”[11]. Jeśli chodzi o architekturę komputerów, to *sensu largo* zgodnie z koncepcją Johna von Neumanna, Johna W. Mauchly'ego i Johna Prespera Eckerta posiadają one:

- procesor (CPU — Central Processing Unit), który składa się z części sterującej i arytmetyczno-logicznej,
- pamięć — (RAM — Random Access Memory) zawierającą dane oraz instrukcje przechowywane w formie cyfrowej,
- urządzenia wejścia/wyjścia (*input/output*)[12].

Współcześnie oprócz CPU i pamięci operacyjnej w skład komputerów wchodzą z reguły takie elementy, jak płyta główna zawierająca m.in. złącza pamięci, karty rozszerzeń, dyski czy urządzenia peryferyjne, koprocesor graficzny (GPU — Graphcial Processing Unit), klawiatura, mysz, pamięć masowa (np. HDD — Hard Disk Drive), napędy dyskowe oraz monitor[13]. Jak wspomniano wyżej, funkcjonowanie komputera opiera się na odpowiednim oprogramowaniu, które można zdefiniować ogólnie jako „zbiór programów, które pozwalają na wykonywanie przez komputer pewnych zadań”. Sam *program* jest natomiast „algorytmem zapisanym w języku zrozumiałym dla komputera”[14]. Na tej podstawie można więc stwierdzić, iż na system komputerowy składają się zarówno

[10] W.A. Sabin: *Glossary of Computer Terms*. MacGraw-Hill Companies 2011, s. 5—6: www.mhhe.com/business/buscom/gregg/docs/appd.pdf; dostęp: 1.08.2013.

[11] J. Kluczewski: *Kurs informatyki dla szkół średnich*. Gdańsk 2000: www.staff.amu.edu.pl/~psi; dostęp: 1.08.2013.

[12] Za P. Dudzik, A. Guzik: *Architektury komputerów i procesorów*. AGH Kraków, 06.07.2011: http://ai.ia.agh.edu.pl/wiki/_media/pl:dydaktyka:miw:2011:architektury_komputerow_v1_1.pdf; dostęp: 1.08.2013. Szerzej: Fulmański, Sobieski, 2004: 69—83.

[13] *Computer*. Techterms.com: www.techterms.com/definition/computer; dostęp: 1.08.2013.

[14] J. Kluczewski: *Kurs informatyki dla szkół średnich*…, op.cit.

oprogramowanie (*software*), jak i zbiór wszystkich jego urządzeń i elementów (*hardware*)[15].

Drugim fundamentalnym elementem składowym cyberprzestrzeni są sieci komputerowe. Za Piotrem Sienkiewiczem i Tomaszem Gobanem-Klasem (1999: 25—26) można je scharakteryzować jako:

> system, który tworzą wzajemnie połączone autonomiczne komputery zdolne do wymiany informacji między sobą. Połączenia w sieci mogą być realizowane za pomocą łączy przewodowych, radiowych, radioliniowych, mikrofalowych, światłowodowych i satelitarnych. Sieci komputerowe budowane są w celu zapewnienia użytkownikom dostępu do wszystkich programów, danych i innych zasobów obliczeniowych niezależnie od przestrzennej lokalizacji użytkowników i tych zasobów, a także dla łatwości aktualizacji informacji w odległych bazach danych i uzyskania wysokiej niezawodności przez stworzenie alternatywnych dróg sięgania do zasobów komputerowych.

Najczęściej dzieli się je na sieci lokalne (LAN — Local Area Network), miejskie (MAN — Metropolitan Area Network) obejmujące obszar kilkudziesięciu kilometrów oraz rozległe (WAN — Wide Area Network) (Ibidem). Czasami występuje też podział na sieci publiczne, będące pod kontrolą dostawcy usług internetowych, który oferuje je osobom prywatnym lub przedsiębiorstwom opłacającym abonament. Występują też sieci prywatne, które są wykorzystywane przez pojedyncze organizacje bądź jednostki (Comer, 2004: 215—225). W szerokim rozumieniu wszystkie sieci komputerowe zawierają się w pojęciu sieci telekomunikacyjnych, które za *Ustawą z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (Dz.U. nr 171, poz. 1800, z późn. zm.) można zdefiniować jako

> systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

Warto jeszcze wspomnieć o dwóch ważnych terminach. Pierwszym są *systemy teleinformatyczne*, na gruncie polskim zdefiniowane w *Ustawie z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną*. Uznano je za

> zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla

[15] Ibidem.

danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu *Ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne* (Dz.U. nr 171, poz. 1800, z późn. zm.)[16].

Krzysztof Liderman (2012: 30) wyróżnił pięć elementów systemu teleinformatycznego:

- informację, która jest przetwarzana, przechowywania i przesyłana,
- urządzenia umożliwiające te działania, czyli komputery, pamięci zewnętrzne, łącza transmisji danych, routery, koncentratory itd.,
- elementy programowe, w tym systemy operacyjne, oprogramowanie narzędziowe czy aplikacje,
- infrastrukturę, czyli budynki, zasilanie (np. energetyczne) bądź systemy ochrony przed nieuprawnionym dostępem fizycznym,
- operatorów, którzy korzystają z możliwości oferowanych przez system, oraz administratorów technicznych.

W kontekście cyberprzestrzeni często wykorzystuje się ponadto pojęcie *sieci teleinformatycznych*. Według *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* (Dz.U. z 1999 r., nr 11, poz. 95, s. 3), rozumie się przez to „organizacyjne i techniczne połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi".

Znając definicje podstawowych kategorii zaliczanych do cyberprzestrzeni, warto wskazać na jej najistotniejsze z punktu widzenia celu badawczego właściwości techniczne. Na wstępie należałoby pokrótce omówić niektóre zasady funkcjonowania jej rdzenia, czyli Internetu, będącego „siecią sieci". Przede wszystkim należy podkreślić, iż jego działanie w wymiarze technicznym opiera się głównie na routerach, które pośredniczą w wymianie danych między sieciami wykorzystującymi różne technologie, media czy schematy adresowania. Routery przekazują pakiety danych pomiędzy sieciami komputerowymi, które składają się na Internet, stanowiąc swoiste bramy, dzięki którym użytkownik jednej sieci jest w stanie korzystać z danych i zasobów znajdujących się w innej, mającej odmienne właściwości techniczne. Urządzenia do nich podłączone określa się mianem stacji sieciowych. Funkcjonowanie Internetu jako jednolitego systemu komunikacyjnego mimo różnorodności na poziomie fizycznej infrastruktury zapewniają protokoły komunikacyjne — stos protokołów TCP/IP (Comer, 2012: 355—360). Składa się on z czterech warstw[17]: warstwy dostępu do sieci, war-

[16] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*. Dz.U. z 2002 r., nr 144, poz. 1204, s. 3.

[17] Istnieje też model siedmiowarstwowy OSI/ISO. Ponadto warto zaznaczyć, że część badaczy wyróżnia też model pięciowarstwowy, dodając pierwszą warstwę fizyczną. Zob. Comer, 2012: 361; Z. Lipiński: *Sieci komputerowe. Model DoD TCP/IP. Rodzina protokołów TCP/IP*. Instytut Matematyki i Informatyki, Uniwersytet Opolski: www.math.uni.opole.pl/~zlipinski/skW/SieciKomp-07-TCP-IP.pdf; dostęp: 9.08.2014; Y.-J. Le Boudec: *The TCP/IP Architecture*.

stwy internetowej, warstwy transportowej oraz warstwy aplikacji. Warstwa internetowa odpowiada za wybór najlepszej drogi dla pakietów danych, warstwa transportowa określa komunikaty i procedury zapewniające skuteczność transferu danych (Comer, 2012: 361—362). Tak więc mimo że Internet jest traktowany jako medium jednolite, z perspektywy technicznej jest on zbiorem rozmaitych stacji sieciowych i sieci komputerowych, połączonych za pomocą routerów oraz innych urządzeń i elementów składających się na globalną infrastrukturę teleinformatyczną (Ibidem, s. 473).

Po drugie, o czym wspomniano już wyżej, cyberprzestrzeń ma charakter niematerialny, choć jest osadzona w materialnej infrastrukturze teleinformatycznej i od niej uzależniona. Infrastruktura ta obejmuje sprzęt komputerowy, media transmisyjne[18], wszystkie urządzenia elektroniczne posiadające określoną masę, właściwości techniczne oraz lokalizację geograficzną. Zdecydowanie bardziej skomplikowana jest natomiast niematerialna natura cyberprzestrzeni. Z jednej strony wiąże się ona z promieniowaniem elektromagnetycznym charakterystycznym dla pracy urządzeń elektronicznych[19], z drugiej strony według wielu przytoczonych wyżej opinii cyberprzestrzeń utożsamiana jest z rzeczywistością wirtualną. Warto w tym kontekście przywołać słowa Andrzeja Filipa:

> W powszechnym użyciu jest […] pojmowanie wirtualnej rzeczywistości rozumianej jako doświadczanie sztucznego środowiska poprzez bodźce zmysłowe, gdzie akcje użytkownika determinują to, co się dzieje w tymże środowisku. […] Według tego podejścia każdy stworzony przez komputer świat jest rodzajem wirtualnej rzeczywistości[20].

Każda akcja podejmowana za pomocą urządzenia wykorzystującego technologie komputerowe, czyli wydanie określonej instrukcji, wykorzystanie programu

---

École Politechnique Fédérale de Lausanne, Fall 2009: http://icawww1.epfl.ch/cn2/0910/slides/1.archi.pdf; dostęp: 9.08.2014.

[18] Media transmisyjne można podzielić na przewodowe i bezprzewodowe. Ze względu na rodzaj wykorzystywanej energii wyróżnia się media elektryczne, radiowe i stosujące transmisję światła. Media transmisyjne przewodowe obejmują okablowanie miedziane oraz włókna światłowodowe, które przesyłają sygnały według wcześniej określonego toru. Bezprzewodowe nie mają takiej ścieżki. Media wykorzystujące energię elektryczną można podzielić na kabel współosiowy oraz skrętkę. Światło do transmisji wykorzystują włókna światłowodowe, podczerwień oraz laser. Wyróżnia się także media wykorzystujące fale elektromagnetyczne, które dzieli się na radio naziemne oraz transmisję satelitarną. Pierwsza i trzecia grupa (media elektryczne oraz radiowe) mogą być zakłócane przez promieniowanie elektromagnetyczne. Za: Comer, 2012: 141—143.

[19] Szerzej na ten temat: Nachev, 2000; *Cyber Electromagnetic*, 2014.

[20] A. Filip: *Wirtualna rzeczywistość czy wirtualny świat?* Centrum Zdalnego Nauczania Uniwersytetu Jagiellońskiego, 23.12.2008: www.czn.uj.edu.pl/index.php/pl/artykuly/wirtualna_rzeczywisto_czy_wirtualny_wiat; dostęp: 1.08.2013.

użytkowego bądź aplikacji rozrywkowej ma więc dwa aspekty — materialny i niematerialny. Jak wspomniano, pierwszy zawiera się w interakcji użytkownika z interfejsem komputera, np. za pomocą klawiatury, myszki oraz monitora. Drugi aspekt, niematerialny, dotyczy już poziomu wykonywanych przez komputer działań arytmetycznych i logicznych. Istota cyberprzestrzeni jest zatem co prawda niematerialna, opiera się jednak na świecie materialnym. Świadomość tej dwuaspektowości ma fundamentalne znaczenie, szczególnie dla analizy pojawiających się w niej zagrożeń dla bezpieczeństwa państw. Warto w tym kontekście przytoczyć słowa Marka Madeja (2009: 29), który w następujący sposób scharakteryzował tę kwestię:

> działania […] wymierzone w bezpieczeństwo jakiegokolwiek państwa lub konkretnego podmiotu albo przynajmniej na nie wpływające (bezpośrednio lub pośrednio) można zainicjować w zasadzie z każdego miejsca na świecie. Jedynym wymogiem jest techniczna możliwość włączenia się do sieci, wejścia do cyberprzestrzeni. Co więcej, przy obecnym kształcie tego środowiska […] poszczególne urządzenia, podłączone w danej chwili do sieci (*host*) mają, niezależnie od swojej geograficznej lokalizacji, relatywnie szybki i równoprawny (tzn. o identycznym zakresie jak inni uczestnicy o tym samym statusie) dostęp do pozostałych elementów układu. Tym samym każdą akcję szkodliwie wpływającą na systemy komputerowe jakiegokolwiek państwa można równie skutecznie przeprowadzić z jego własnego terytorium, jak i z obszaru położonego w zupełnie innej części globu.

Trzecia istotna cecha cyberprzestrzeni wynika z jej otwartej architektury, co pokrótce omówiono przy okazji charakterystyki rewolucji informatycznej. Warto tu jednak szerzej scharakteryzować kilka zagadnień. Przede wszystkim architektura cyberprzestrzeni jest niezwykle rozproszona. Jak wspomniano, jej centrum, czyli najważniejszą częścią składową, jest Internet, który oplata swoim zasięgiem cały świat. Do tego należy doliczyć szereg innych elementów, takich jak odrębne sieci komputerowe oraz komputery offline. Ten rozproszony charakter cyberprzestrzeni składającej się z niewyobrażalnej liczby elementów jest zarazem negatywną i pozytywną cechą. Z jednej strony, o czym już wspomniano, takie rozwiązania sprawiają, że awaria jednego, a nawet wielu węzłów sieci nie sparaliżuje całej cyberprzestrzeni (zob. Labovitz, Ahuja, Jahanian, 1998). Sygnał cyfrowy dzięki obecnej architekturze zawsze powinien znaleźć drogę do miejsca przeznaczenia, omijając uszkodzone obszary. Tym samym jest to czynnik, który działa stabilizująco na funkcjonowanie przestrzeni teleinformatycznej. Z drugiej jednak strony otwarta architektura oznacza zarazem mnogość wejść, „bram" do całego systemu, dostęp do cyberprzestrzeni jest bowiem możliwy nie tylko dzięki komputerom stacjonarnym czy notebookom, ale także innym pokrewnym urządzeniom elektronicznym, posiadającym cechy komputera. Jak zauważono wcześniej, najlepiej świadczy o tym liczba istniejących obecnie na

świecie telefonów komórkowych, z których zdecydowana większość ma możliwość połączenia się z Internetem. Taka sytuacja może utrudniać zwalczanie incydentów teleinformatycznych. Problematyczne bywa np. zidentyfikowanie sprawcy cyberataku, który umiejętnie wykorzystał potencjał technologii Wi-Fi[21]. Ponownie warto odwołać się tu do słów Marka Madeja (2009: 30—31), który ujął te kwestie następująco:

> Podstawowe reguły określające metody i sposób przedstawienia oraz transferu danych w Internecie nie zostały […] sformułowane z uwzględnieniem niebezpieczeństw grożących sieci i wpływających na jej funkcjonowanie od wewnątrz. Z tego powodu nie pozwalają one na jednoznaczną i każdorazową (tzn. wykonalną niezależnie od momentu podjęcia takiej próby) identyfikację podmiotu dokonującego danej operacji […] ani też nie wymagają obowiązkowej autoryzacji dostępu do systemu. Dodatkowo te i tak ograniczone możliwości ustalenia sprawców poszczególnych działań w cyberprzestrzeni redukuje jeszcze sama skala i złożoność wykonywanych dziś jednocześnie transferów danych.

Po czwarte: warto pamiętać, iż prawidłowe funkcjonowanie cyberprzestrzeni jest ściśle uzależnione od niezawodności infrastruktury teleinformatycznej. Sprawność kabli, światłowodów, routerów czy stacji przekaźnikowych ma zasadnicze znaczenie dla jej istnienia. W tym kontekście należy zauważyć, iż jakkolwiek sama architektura przestrzeni teleinformatycznej jest rozproszona, to mimo wszystko na świecie wykształciły się pewne „wąskie gardła", przez które przechodzi większość ruchu w sieci. Co prawda nawet one mogą być ominięte w wypadku awarii, wiązałoby się to jednak ze znacznym spowolnieniem działania Internetu. Jest to szczególnie widoczne, jeśli spojrzy się na położenie oplatających Ziemię światłowodów, które stanowią szkielet Internetu. Wbrew pozorom zdecydowana większość ruchu w nim, dzięki omówionej już inicjatywie FLAG, odbywa się współcześnie nie za pomocą łączności satelitarnej, lecz kabli zlokalizowanych na dnie oceanów. Na tym tle do „wąskich gardeł" należy zaliczyć m.in. Nowy Jork, gdzie zbiega się większość światłowodów przesyłających ruch internetowy z Europy, Afryki oraz Ameryki Południowej i Karaibów. Inne istotne to Cieśnina Ormuz, Tajpej, Hong Kong, Tokio, Guam, Manila, Kanał La Manche, Cieśnina Gibraltarska oraz Miami[22]. O głębokim uzależnieniu funkcjonalności rdzenia cyberprzestrzeni od sprawności infrastruktury teleinformatycznej świadczy najlepiej szereg incydentów, które miały miejsce w jednym z największych

[21] Chodzi tu nie tyle o techniczne trudności związane z wykryciem źródła włamania, co z identyfikacją sprawcy, który podłączył się do obcej, np. publicznej sieci Wi-Fi na czas dokonania przestępstwa. Niektórzy eksperci taki proceder nazywają mianem *wireless hacking*. Zob. D. Chick: *Wireless Network Attackers*. The Network Administrator: www.thenetworkadministrator.com/wardriving.htm; dostęp: 12.08.2014.

[22] Zob. *Submarine Cable Map*: www.submarinecablemap.com/#; dostęp: 6.12.2013.

wąskich gardeł światowej sieci światłowodowej — w okolicach Morza Czerwonego i Kanału Sueskiego. Już w styczniu 2008 roku doszło tam do dwóch awarii: najpierw kabla FALCON (będącego częścią FLAG) łączącego Indie z krajami Zatoki Perskiej, a w tydzień później, 30 stycznia, doszło do uszkodzenia systemu światłowodów SEA-ME-WE 4 oraz FLAG Telecom w pobliżu Aleksandrii. W ich wyniku miała miejsce jedna z najpoważniejszych awarii Internetu w historii, która objęła zasięgiem m.in. Egipt, Indie, Bahrajn, Afganistan, Bangladesz, Kuwejt, Malediwy, Pakistan, Arabię Saudyjską i Zjednoczone Emiraty Arabskie. Najpoważniejszą postać przybrały problemy w Egipcie, gdzie zostało zablokowane ok. 70% ruchu sieciowego, i w Indiach, gdzie zablokowane było ok. 50%. W sumie ucierpiało z tego powodu ponad 86 mln internautów, w tym aż 60 mln w Indiach i 12 mln w Pakistanie[23]. Na początku lutego 2008 roku doszło do kolejnych uszkodzeń, a co za tym idzie do ponownego paraliżu Internetu. Awarie nastąpiły na odcinku kabla FALCON między Omanem a Zjednoczonymi Emiratami Arabskimi (został zniszczony przez kotwicę), w systemie DOHA-HALOUL między Katarem a ZEA oraz SEA-ME-WE-4 w pobliżu Malezji[24]. Poważne awarie podwodnych kabli skutkujące zaburzeniami funkcjonowania głównego rdzenia cyberprzestrzeni nastąpiły także 19 grudnia 2008 roku, gdy przecięte zostały systemy kabli FLAG Telecom, SEA-ME-WE-3 oraz SEA-ME-WE-4, które łączyły Egipt, Sycylię oraz Maltę. W wyniku tych awarii tylko w Egipcie o 80% obniżyła się przepustowość Internetu, utrudnione było także wykonywanie połączeń telefonicznych między Europą a Bliskim Wschodem i Azją[25]. Takich wydarzeń, wynikających zarówno z działań człowieka (głównie źle opuszczane kotwice oraz sieci rybackie), jak i natury (sztormy, tajfuny, trzęsienia ziemi), było w ostatnich latach zdecydowanie więcej. Wszystkie one udowodniły, iż funkcjonowanie Internetu, czyli głównego nurtu cyberprzestrzeni, jest uzależnione od sprawności elementów, które są często przez badaczy niedoceniane. Istnienie tych „wąskich gardeł" Internetu stanowi poważną słabość techniczną, która może być interpretowana jako jedno z wyzwań dla bezpieczeństwa międzynarodowego. Jest to tym wyraźniejsze, iż — jak zwrócił uwagę Bobbie Johnson — działalność systemu DNS opiera się jedynie na 13 serwerach

[23] A.A. Zain: *Cable damage hits one million Internet users in UAE*. „Khaleej Times" 04.02.2008: www.khaleejtimes.com/DisplayArticleNew.asp?section=theuae&xfile=data/theuae/2008/february/theuae_february121.xml; dostęp: 2.08.2013.

[24] *Update on Submarine Cable Cut Repairs*. Daily Bulletin, FLAG Telecom, 07.02.2008: http://web.archive.org/web/20080208124925/http://www.flagtelecom.com/index.cfm?channel=4328&NewsID=27493; dostęp: 2.08.2013; *4th Undersea Cable Break: Between Catar and UAE*. Mathaba, 04.02.2008: http://mathaba.net/news/?x=580660; dostęp: 2.08.2013; A.A. Zain: *Cable damage hits one million Internet users*, op.cit.

[25] *Severed cable disrupts net access*. BBC News, 19.12.2008: http://news.bbc.co.uk/2/hi/technology/7792688.stm; dostęp: 2.08.2013; J. Regan, *UPDATE 3-Undersea cable breaks out Internet in Mideast, Asia*. Reuters, 20.12.2008: www.reuters.com/article/2008/12/20/us-internet-idUSTRE4BJ0FV20081220; dostęp: 2.08.2013.

(*root name servers*), które odpowiadają za cały ruch w sieci. Co prawda są one geograficznie rozproszone, gdyż znajdują się aż w 376 miejscach na świecie, nadal jednak istnieje możliwość sparaliżowania ich pracy, co mogłoby utrudnić funkcjonowanie globalnego Internetu[26].

Należy ponadto podkreślić, iż istotną cechą techniczną charakteryzującą cyberprzestrzeń jest pole elektromagnetyczne, właściwe zarówno dla komputerów, telefonów komórkowych, jak i routerów Wi-Fi czy nawet urządzeń Bluetooth. Z jednej strony jest to czynnik, który może negatywnie wpływać na zdrowie osób korzystających z dobrodziejstw tej domeny[27], z drugiej jednak jest to także istotna cecha z punktu widzenia bezpieczeństwa, warto bowiem zauważyć, iż występowanie pola elektromagnetycznego od lat jest wykorzystywane przez wojsko, które opracowało różnorodne rodzaje broni oparte na impulsie elektromagnetycznym. Indukując wysokie napięcie w sieciach i urządzeniach elektronicznych lub elektrycznych, powoduje wydzielanie się dużych ilości ciepła, a w konsekwencji ich uszkodzenie bądź zniszczenie. Tego typu uzbrojenie ma w dobie rewolucji informatycznej rosnące znaczenie, na co zwrócili uwagę Tomasz Szubrycht i Tomasz Szymański (2005: 122, 133—134). Według nich

> wytworzony impuls elektromagnetyczny uniemożliwi pracę biur i banków, powrót do domu, a nawet wyjście z windy. Przedstawiana broń jest bronią doskonałą. W wyniku jej użycia nie będzie żadnych zniszczeń, ognia, zabitych, rannych, a i tak efekty okażą się zatrważające. W ciągu sekundy przyniesie ona ciemność, chaos, bezsilność i zdumienie. Sprzęt informatyczny jest szczególnie narażony na Electromagnetic Pulse (EMP). Wynika to z faktu, iż większość współczesnych urządzeń elektronicznych oparta jest na technologii półprzewodników tlenkowych (Metal Oxide Semiconductor — MOS), tym samym są one podatne na impulsy wysokonapięciowe. Na takie oddziaływanie narażone są również urządzenia telekomunikacyjne, ze względu na miedziane połączenia (okablowanie), oraz radary, satelity i wiele innych urządzeń elektronicznych powszechnie wykorzystywanych zarówno na współczesnym polu walki, jak i w życiu codziennym.

[26] W lutym 2013 roku operatorami *root name servers* byli: VeriSign, Inc., Information Sciences Institute, Cogent Communications, University of Maryland, NASA Ames Research Center, Internet System Consortium, Inc., U.S. DOD Network Information Center, U.S. Army Research Lab, Netnod, RIPE NCC, ICANN oraz WIDE Project. Zob. B. Johnson: *Faulty cable blacks out internet for milions*. „The Guardian" 31.01.2008: www.theguardian.com/technology/2008/jan/31/internet.blackout.asia; dostęp: 2.08.2013; *Root servers*. Root.servers.org: www.root-servers.org; dostęp: 2.08.2013.

[27] *Fakty i mity o promieniowaniu elektromagnetycznym*. „Komputer Świat" 08.11.2010: www.komputerswiat.pl/jak-to-dziala/2010/11/fakty-i-mity-o-promieniowaniu-elektromagnetycznym.aspx; dostęp: 2.08.2013.

Rozważania te podsumowali autorzy następująco:

> Niezależnie od użycia bądź nie takiego rodzaju broni trzeba pamiętać, że w wysoko rozwiniętych społeczeństwach uzależnienie od elektroniki staje się swoistą piętą achillesową. Wykorzystanie EMP jest szczególnie efektywne w stosunku do wysoce uprzemysłowionych państw, ponieważ cechuje je duża koncentracja urządzeń elektronicznych.

Na tym tle widać więc wyraźnie, iż cyberprzestrzeń posiada niezwykle skomplikowany charakter techniczny, co wynika zarówno z liczby składających się na nią elementów, wielowymiarowości, niematerialności i „aterytorialności", otwartej architektury, jak i promieniowania elektromagnetycznego. Wzięcie pod uwagę wszystkich tych cech jest jednak warunkiem *sine qua non* zrozumienia, jaka jest istota przestrzeni teleinformatycznej jako nowej domeny rywalizacji i współpracy państw.

2.3. Cechy cyberprzestrzeni jako nowego wymiaru bezpieczeństwa państw

Na podstawie powyższych rozważań można przejść do omówienia szeregu istotnych powodów, które sprawiają, że cyberprzestrzeń współcześnie jest nie tylko domeną, która przynosi całej ludzkości określone profity, ale również, ze względu na swój charakter, stanowi poważne zagrożenie dla bezpieczeństwa w różnych ujęciach[28].

Od lat trwa ożywiona dyskusja naukowa poświęcona temu, co sprawia, że cyberprzestrzeń staje się w coraz większym stopniu domeną szkodliwej aktywności różnorodnie motywowanych podmiotów. W ciekawy sposób ujął to Fred Schreier, który wyróżnił trzy grupy powodów tego stanu rzeczy. Przede wszystkim natura zagrożeń w tej sferze jest jego zdaniem tak szeroka, jak sama cyberprzestrzeń. Oznacza to, że każdy aspekt życia człowieka, który jest zależny od sieci, jednocześnie ponosi ryzyko. Po drugie według Schreiera (2015: 32—33) wyzwania wynikające z istnienia cyberprzestrzeni są w niej głęboko osadzone. Oznacza to, że wywodzą się one z problemów technicznych dla niej właściwych, czyli np. błędnych instrukcji w oprogramowaniu, wadliwych systemów operacyjnych, zepsutego sprzętu czy funkcjonowania wirusów oraz trojanów.

[28] Jak pisała Myriam Dunn-Cavelty (2008: 42), „cyberzagrożenia wywodzą się ze szkodliwego wykorzystania technologii informacyjnych i komunikacyjnych".

Po trzecie zagrożenia te są niezwykle zróżnicowane, co jest uzależnione od bogactwa podmiotów wykorzystujących technologie teleinformatyczne, w sieci działają bowiem hobbyści, wandale, ekstremiści polityczni i religijni, grupy przestępcze, najemnicy, hakerzy, haktywiści czy wreszcie państwa oraz ich organizacje. Można tu również przywołać słowa Johna Arquilli oraz Davida Ronfeldta (2001: 1—2), którzy zauważyli, iż rewolucja informatyczna zmieniła naturę konfliktów we wszystkich wymiarach. Ich zdaniem szczególnie istotne są tu dwa procesy. Po pierwsze postęp technologiczny z zasady wzmacnia sieciowe formy organizacji, dając im przewagę nad tymi tradycyjnymi, hierarchicznymi, a co za tym idzie potęga stopniowo „przesuwa się" w stronę aktorów niepaństwowych, którzy są w stanie działać w sposób sieciowy. Po drugie nigdy wcześniej wiedza i *soft power*, czyli przede wszystkim ICT, nie były tak istotne dla przebiegu i wyników konfliktów. Nieco inaczej podeszli do tego Richard A. Clarke i Robert K. Knake (2010: 73—74), którzy powodów pojawienia się fenomenu cyberwojny upatrywali w trzech grupach czynników: błędach w fazie projektowania Internetu, błędach w oprogramowaniu oraz sprzęcie komputerowym, a także w tendencji do podłączania coraz większej liczby krytycznych systemów do globalnej sieci. W ciekawy sposób odniósł się do tych zagadnień także Kenneth Geers (2011: 24), który wśród powodów znacznej wrażliwości systemów komputerowych na szkodliwe działania wymienił m.in. monokulturowość środowiska komputerowego, wysokie koszty produkcji oprogramowania wysokiej jakości, techniczne trudności związane z publikacją łat (*patch*) dla programów czy wykorzystanie praw administratora przez zwykłe aplikacje.

Na tej podstawie warto spróbować wyróżnić szereg cech, które determinują charakter cyberprzestrzeni jako nowego wymiaru bezpieczeństwa państw. Przede wszystkim, o czym wspomniano wyżej, jest to przestrzeń niematerialna, w której kategorie znane ze świata fizycznego nie obowiązują, przynajmniej w niezmienionej formie. Wielu autorów słusznie wskazuje, iż jest to przestrzeń „aterytorialna" i „ageograficzna". Kenneth Geers (2011: 10) stwierdził na przykład, iż „w cyberkonflikcie dystans lądowy między przeciwnikami może być nieistotny", gdyż w sieci wszyscy sąsiadują ze wszystkimi, a zatem choć infrastruktura teleinformatyczna posiada określoną lokalizację, to atak w cyberprzestrzeni nie przekracza żadnych granic. W sensie materialnym może się zamanifestować w zasadzie w dwóch sytuacjach. W pierwszej, najprostszej, wiązałby się ze zniszczeniami fizycznymi. W takim przypadku związek przyczynowo-skutkowy między włamaniem a przekroczeniem określonych granic terytorialnych oraz naruszeniem własności jest oczywisty. W drugiej, o wiele częstszej sytuacji, cyberatak skutkuje manipulacją danymi znajdującymi się na określonym komputerze. Jako że komputer ma przynależność prawną i lokalizację geograficzną, można wskazać na pośrednią relację między cyberprzestrzenią a wymiarem fizycznym. Bez względu na to sama niematerialność

tej domeny rodzi zasadnicze wątpliwości natury prawnej i politycznej. Przede wszystkim powstaje pytanie: czy i jakie cyberataki stanowią naruszenie zakazu stosowania siły w stosunkach międzynarodowych. Po drugie: czy mogą być one kwalifikowane jako akt wojny (w przypadku działań państw lub organizacji międzynarodowych). Po trzecie: w jaki sposób interpretować działania w sieci w sytuacji, w której identyfikacja sprawców jest trudniejsza i jakościowo odmienna od wymiaru fizycznego (zob. Buffalini, 2012: 89—109; Ellis, 2001; Kanuck, 2009: 1571—1597; Sandvik, 2012). Po czwarte: jak się mają te zagrożenia do takich kategorii, jak integralność terytorialna czy suwerenność polityczna. Tego typu wątpliwości powstających na styku nowych technologii oraz mechanizmów politycznych i prawnych współcześnie pojawia się coraz więcej.

Druga cecha cyberprzestrzeni jako nowego wymiaru bezpieczeństwa jest szczególnie związana z jedną z wymienionych wyżej wątpliwości — kwestią identyfikacji sprawców (Roscini, 2010: 96—102; Lipson, 2002). Sfera ta, mając charakter niematerialny, sprawia, iż zachowanie anonimowości jest znacząco ułatwione, cyberatak na infrastrukturę teleinformatyczną może zostać bowiem potencjalnie przeprowadzony z każdego miejsca globu, z komputerów podłączonych np. do publicznej sieci Wi-Fi lub skutecznie zakamuflowanych np. wykorzystaniem sieci *botnet* lub TOR (*The Onion Router*[29]). W tej sytuacji samo rozpoznanie komputera, z którego przeprowadzono atak, jest sprawą niezwykle trudną. Nawet realizacja tego zadania nie oznacza, iż identyfikacja sprawcy będzie udana, z reguły bowiem nie istnieje możliwość sprawdzenia, kto w rzeczywistości siedział za pulpitem komputera. Trudności ze wskazaniem osoby odpowiedzialnej za aktywność przestępczą w cyberprzestrzeni mają więc charakter dwuwymiarowy. Jest to czynnik sprzyjający jej wykorzystaniu w charakterze nowej sfery realizowania interesów przez różnorodne podmioty, począwszy od jednostek, kończąc na państwach i ich organizacjach (Finklea, Theohary, 2012: 1—7; Lakomy, 2011a: 156).

Trzecia istotna cecha cyberprzestrzeni wiąże się z niskimi kosztami „wejścia", działania w niej. Aby zrozumieć to zagadnienie, warto najpierw odwołać się do okresu zimnej wojny, kiedy równowagę strategiczną między mocarstwami zachowywało się za sprawą niezwykle wysokich nakładów na zbrojenia. To dzięki kosztownej rozbudowie zarówno potencjału konwencjonalnego, jak i broni masowego rażenia, rywalizujące bloki zachowywały zdolność do dokonania strategicznego uderzenia na terytorium przeciwnika (Sokolski, red., 2004). Tymczasem, jak zauważono np. w raporcie RAND z 1996 roku, w dobie rewolucji informatycznej, strategiczny atak na Stany Zjednoczone może być dokonany za pomocą kosztującego nieporównanie mniej złośliwego oprogramowania

[29] Szerzej na temat sieci TOR: Saramak, 2014: 192—195.

(*malware*)[30]. Zdobycie wirusów, robaków, trojanów jest współcześnie zadaniem niezwykle prostym. W sieci mniej lub bardziej otwarcie funkcjonują tysiące stron, na których za darmo można pobrać starsze i mniej szkodliwe modele, jak i te najnowsze, niepodatne na działanie programów antywirusowych i innych zabezpieczeń. Stosunkowo łatwo można także uzyskać wiedzę na temat aktualnych luk w zabezpieczeniach wielu popularnych programów oraz metod ich wykorzystania do włamań. Również samo opracowanie nowych sposobów ataków, specjalistycznego oprogramowania, odpowiedzialnego np. za kontrolowanie sieci *botnet*, mimo wysokiego poziomu skomplikowania jest zdecydowanie tańsze i szybsze niż rozwój konwencjonalnych technologii wojskowych. Działania w cyberprzestrzeni nie wymagają więc z reguły ani wysokich i długotrwałych nakładów finansowych, ani tysięcy zaangażowanych osób, porównywalne zagrożenie może bowiem stanowić jednostka posiadająca dostęp do komputera podłączonego do sieci. Jeśli jest ona odpowiednio uzdolniona i posiada właściwe narzędzia, jest w stanie przeprowadzić skuteczny cyberatak (Schreier, 2015: 12). Jest to więc czynnik, który zdecydowanie ułatwia wykorzystanie cyberprzestrzeni jako nowej domeny realizacji własnych interesów zarówno przez państwa, jak i inne, niepaństwowe podmioty, w tym np. organizacje terrorystyczne czy grupy przestępcze. Trafnie te zagadnienia podsumowali Roger C. Molander, Andrew S. Riddile i Peter A. Wilson (1996: 17—19), porównując globalny Internet do XIX-wiecznego Dzikiego Zachodu:

> W tej sytuacji wiele zaawansowanych i wzajemnie połączonych sieci może stać się celem ataków, przeprowadzonych przez szerokie spektrum podmiotów, w tym uzdolnionych jednostek, aktorów niepaństwowych, takich jak transnarodowe grupy przestępcze oraz państw, posiadających wyszkolone kadry „cyberwojowników". […] W swojej istocie Internet posiada część cech obszaru otwartego dla wypasu bydła pod koniec XIX wieku. Ta metafora „Dzikiego Zachodu" jest trafna, jako że trwa dyskusja nad tym, czy użytkownicy Internetu powinni łatwo zdobyć cyberprzestrzenny odpowiednik drutu kolczastego — ochronę dla baz danych poprzez techniki szyfrowania.

Rezultatem tych tendencji stała się zdaniem autorów sytuacja, w której za cyberatakiem może stać dosłownie każdy.

Po czwarte, jak zauważono w raporcie RAND, cyberprzestrzeń stała się dogodnym obszarem działań także ze względu na brak systemów wczesnego ostrzegania, oceny prawdopodobieństwa ataków oraz wywiadu strategicznego. Odnosząc się do przytoczonego już przykładu zimnej wojny, należy wskazać, że wszelkie działania militarne podejmowane wówczas przez rywalizu-

[30] Przez szeroko pojęte złośliwe oprogramowanie David S. Wall rozumiał „skrypty, których celem jest zakłócenie, uszkodzenie lub kradzież informacji z systemów komputerowych". Zob. *Strategic War*, 1996; Wall, 2007: 225.

jące ze sobą bloki były w jakimś stopniu dostrzegalne przez drugą stronę. Czy to dzięki działaniom wywiadowczym, czy systemom wczesnego ostrzegania, rządy państw posiadały, niepełną co prawda, wiedzę na temat kierunku działań przeciwnika, jego możliwych zamiarów i potencjału. Tymczasem w cyberprzestrzeni powielenie tych mechanizmów jest w zasadzie niemożliwe. Wynika to zarówno z łatwej do osiągnięcia anonimowości, jak i braku technicznych możliwości stworzenia systemów wczesnego ostrzegania[31]. Istnieje ponadto pewna trudność wstępnego odróżnienia strategicznych ataków w sieci od zwykłej działalności hakerskiej, szpiegowskiej, a czasami nawet typowych awarii niektórych urządzeń. Jak podsumowali to eksperci RAND, w cyberprzestrzeni nie wiadomo, „kim będą twoi przeciwnicy… oraz jakie będą ich intencje i możliwości"[32].

Po piąte: szkodliwemu wykorzystaniu cyberprzestrzeni sprzyja z pewnością charakter rewolucji informatycznej, która objęła niemal wszystkie dziedziny życia na całym świecie. Otworzyło to zupełnie nowe możliwości manipulacji ludźmi i ich zbiorowościami. Trafnie ujął to Martin C. Libicki (2007: 292), który stwierdził: „im gęstsza elektronika oraz im bardziej cyberprzestrzeń przenika realną przestrzeń, tym bardziej realne życie staje się uzależnione od właściwego funkcjonowania cyberprzestrzeni"[33]. Klaus-Peter Saalbach (2013: 4—5) wśród najważniejszych powodów tego stanu rzeczy wymienił:

- pojawienie się NGN (Next Generation Network), w której telewizja, komputery czy telefony przesyłają pakiety danych, korzystając z protokołu internetowego,
- powstanie koncepcji IoT (Internet of Things), polegającej na podłączeniu urządzeń czy nawet określonych dóbr do sieci,
- powszechne zastosowanie w przemyśle systemów ICS (Industrial Control Systems) oraz SCADA (Supervisory Control and Data Acquisition), które umożliwiają wykorzystanie Internetu do komunikacji między maszynami,
- pojawienie się koncepcji sieciocentryczności pola walki,
- planowane wykorzystanie technologii teleinformatycznych do zarządzania domem,
- rozwój koncepcji *smart grid*, polegającej na wykorzystaniu osiągnięć ICT przez sieć elektroenergetyczną,

[31] Oczywiście istnieją systemy określane mianem „systemów wczesnego ostrzegania o zagrożeniach", takie jak np. polski ARAKIS-GOV. Nie jest to jednak system, który potrafi „przewidzieć" nadchodzący atak na takiej zasadzie, jak w opisanym wyżej przykładzie zimnej wojny. Zob. *System ARAKIS-GOV.* CERT.GOV.PL: www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html; dostęp: 21.08.2014.

[32] Zob. *Strategic War* 1996; Molander, Riddile, Wilson, 1996: 26.

[33] Tego typu tendencje w różnych płaszczyznach zauważył o wiele wcześniej Erhard Cziomer (2005: 155), według którego częstokroć występuje pewien „paradoks bezpieczeństwa", który polega na tym, że wykorzystanie określonych środków skutkuje powstawaniem nowych zagrożeń lub nasileniem już istniejących.

- popularyzacja *cloud computingu*, polegającego m.in. na wykorzystaniu Internetu do zdalnego łączenia mocy obliczeniowej komputerów,
- pojawienie się telefonów komórkowych z wbudowaną możliwością lokalizacji za pomocą GPS (Global Positioning System).

Wszystkie te procesy stanowią więc potencjalną szansę dla jednostek i grup posiadających odpowiednie motywacje, umiejętności i środki do cyberataków (Yagil, 2002: 109). Problem ten można zobrazować na przykładzie włamania do banku. Przed nastaniem rewolucji technologicznej proceder ten wymagał obecności przestępcy w określonym miejscu, skrupulatnej organizacji i szeregu niebezpiecznych działań związanych z samym napadem. Współcześnie tego typu akcja może zostać zorganizowana i przeprowadzona z odległości tysięcy kilometrów. Tendencje te są jeszcze bardziej widoczne na szczeblu państwowym. Jak zauważono w raporcie Międzynarodowego Związku Telekomunikacyjnego, wszystkie istotne dla społeczeństw usługi są dziś zdominowane przez technologie ICT. Z jednej strony wymieniono tu takie kwestie, jak zaopatrzenie w wodę, energię elektryczną, funkcjonowanie sieci telefonicznych bądź sterowanie ruchem ulicznym, z drugiej jednak strony rewolucja informatyczna objęła także bardziej „przyziemne" urządzenia, takie jak windy, samochody czy nawet klimatyzację. Zdaniem ITU umożliwia to szkodzenie zbiorowościom ludzkim w sposób dotychczas niespotykany[34]. Ewidentnym przykładem wagi tych procesów jest zmiana sytuacji Stanów Zjednoczonych, które posiadają dogodną pozycję geostrategiczną. W XX wieku zainwestowały one ogromne środki finansowe, aby ich terytorium nie było zagrożone żadnymi działaniami zbrojnymi. W okresie pozimnowojennym dokonanie konwencjonalnego uderzenia na USA wymagałoby ogromnych nakładów finansowych oraz potencjału wojskowego. Nie wzięto jednak pod uwagę pojawienia się cyberprzestrzeni, gdzie tego typu atak jest jak najbardziej możliwy. Jak wspomniano we wstępie, część amerykańskich badaczy obawia się wręcz wystąpienia „elektronicznego Pearl Harbor", strategicznego uderzenia poprzez sieć, które mogłoby złamać gospodarkę USA i sparaliżować instytucje publiczne. Wszystko to dzięki rosnącemu uzależnieniu kraju od infrastruktury teleinformatycznej (Cordesman, Cordesman, 2001: 1—4; Isenberg, Meridian, 2000: 92—103; Lakomy, 2010b: 57—58). Te same tendencje są charakterystyczne również dla sił zbrojnych, które w drugiej połowie XX wieku uzależniły się od różnorodnych urządzeń elektronicznych i sieci telekomunikacyjnych. Podnosząc dzięki temu swą skuteczność w konwencjonalnych działaniach wojennych, jednocześnie stały się podatne na ataki w cyberprzestrzeni. Jak podsumował to Bruce Berkowitz (1997: 219), technologie informacyjne już w latach 90. osiągnęły masę krytyczną, co wpłynęło na osłabienie bezpieczeństwa państw.

[34] Rosnące uzależnienie od ICT może się wiązać np. z negatywnymi konsekwencjami gospodarczymi, rozwój ekonomiczny, szczególnie w państwach rozwiniętych, jest bowiem w coraz większym stopniu uwarunkowany niezawodnością nowych technologii. Zob. *Understanding Cybercrime*, 2012, s. 2.

Kolejną interesującą cechą cyberprzestrzeni jako nowego wymiaru bezpieczeństwa jest zasadnicza trudność współpracy międzynarodowej w tym wymiarze. Z jednej strony, na co uwagę zwracało część amerykańskich badaczy, sieci teleinformatyczne wykorzystywane m.in. do komunikacji między krajami mogą być wrażliwymi celami ataków (*Strategic War*, 1996). Ponadto ochrona sojuszników przed nimi jest zdecydowanie trudniejsza, niż miałoby to miejsce w przypadku konwencjonalnych działań zbrojnych. Z drugiej strony należy wskazać na narastające problemy we współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa (szerzej w rozdziale 5). Mimo ponad dwóch dekad prób społeczność międzynarodowa nadal nie doszła do konsensusu w kwestiach nawet najbardziej podstawowych, nadal nie zdefiniowano m.in. w prawie międzynarodowym, czym jest atak hakerski oraz z jakimi wiąże się konsekwencjami np. w świetle Karty Narodów Zjednoczonych. Co więcej, nadal jedynym z nielicznych ponadregionalnych dokumentów poświęconych zagrożeniom pojawiającym się w przestrzeni teleinformatycznej pozostaje *Konwencja o cyberprzestępczości* Rady Europy z 2001 roku (zob. Skrzypczak, 2011: 51—58; Siwicki, 2013: 80). Fiaskiem kończą się z kolei wszystkie inne próby wprowadzenia globalnych regulacji w tej dziedzinie, w tym np. negocjacje w ramach Międzynarodowego Związku Telekomunikacyjnego[35]. Brak wiążących uzgodnień prawnomiędzynarodowych i zasadniczą trudność współpracy państw w tej dziedzinie należy więc uznać za kolejny czynnik sprzyjający szkodliwemu wykorzystaniu cyberprzestrzeni. Świetnym przykładem tego stanu rzeczy jest *casus* Chin, które oskarżone o działania szpiegowskie w Internecie stwierdziły, iż nie istnieje ustalona w prawie międzynarodowym definicja „ataków hakerskich" oraz brakuje podstaw prawnych do ich odróżnienia od „rutynowego zbierania informacji" w sieci[36].

Warto również zauważyć, iż cyberprzestrzeń faworyzuje działania ofensywne nad defensywnymi (Coleman, 2008). Wynika to z trzech omówionych już wyżej cech: z natury przestrzeni teleinformatycznej, która posiada sprzyjającą anonimowości otwartą architekturę, dlatego trudność wyśledzenia sprawcy ataku oczywiście wzmacnia ofensywną wymowę aktywności w sieci; z niskich

[35] *New global telecoms treaty agreed in Dubai*. International Telecommunication Union, 14.12.2012: www.itu.int/net/pressoffice/press_releases/2012/92.aspx#.UPEuUPLM9p9; dostęp: 4.08.2013; C. Albanesius: *US Refuses to Sign ITU Treaty Over Internet Provisions*. PCMAG, 13.12.2012: www.pcmag.com/article2/0,2817,2413218,00.asp; dostęp: 4.08.2013; C. Albanesius: *UN Control of Web Would 'Open Door to Censorship'*. 06.12.2012: www.pcmag.com/article2/0,2817,2412937,00.asp; C. Arthur: *Internet remains unregulated after UN treaty blocked*. 14.12.2012: www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated; dostęp: 4.08.2013.

[36] *Exposing One of China's Cyber Espionage Units*. Mandiant Report 2012; *Chiny odrzucają oskarżenia o hakerskie ataki w USA*. Wirtualna Polska, 20.02.2013: http://konflikty.wp.pl/kat,1356,title,Chiny-odrzucaja-oskarzenia-o-hakerskie-ataki-w-USA,wid,15348738,wiadomosc.html; dostęp: 11.08.2013.

wymagań „wejścia" do cyberprzestrzeni, co sprawia, iż mogą tam działać nawet podmioty o niskim stopniu zorganizowania, nieposiadające większych zasobów finansowych; z braku systemów wczesnego ostrzegania i wywiadu strategicznego.

W ciekawy sposób ujął to Krzysztof Liedel (2014: 85) według którego

> pierwszym — i jednym z najważniejszych aspektów prowadzenia walki w cyberprzestrzeni — jest to, że każdy, kto posiada łącze internetowe i komputer, może przypuścić atak w cyberprzestrzeni. Oczywiście nie mamy tu na myśli przypuszczenia SKUTECZNEGO ataku — umiejętności, sprzęt i wiedza niezbędne do tego na szczęście nadal nie są aż tak powszechne.

Na tym tle należy więc podkreślić, iż ataki w cyberprzestrzeni przeprowadzane są z ogromną szybkością, mogą być rozproszone i stale ponawiane, obrońcy muszą zatem reagować na bieżąco na włamania, których nie są w stanie wcześniej ani przewidzieć, ani często wykryć[37]. Zablokowanie ich na czas, tak aby nie zdołały poczynić poważniejszych szkód, jest więc niezwykle trudnym wyzwaniem. Jest to tym bardziej skomplikowane, jeśli cyberataki przeprowadzane są na różnych płaszczyznach, z wielu miejsc naraz. Sytuację dodatkowo gmatwa fakt, iż napastnicy działają w środowisku niezwykle bogatym w potencjalne cele. Może to być komputer należący do przedstawiciela władz państwowych, komponent systemu obronnego, finansowego lub sieć elektroenergetyczna (Schreier, 2015: 12—13). O przewadze aspektu ofensywnego nad defensywnym świadczy również to, iż zabezpieczenie państwa przed cyberatakami (np. wymierzonymi w krytyczną infrastrukturę teleinformatyczną) w przeciwieństwie do ich organizowania wiąże się z wysokimi nakładami finansowymi oraz z wysiłkiem organizacyjnym i technologicznym[38].

Cyberprzestrzeń jest także obszarem, w którym istnieje zasadnicza trudność odstraszenia potencjalnego przeciwnika, nie istnieje tu bowiem odpowiednik

---

[37] Przy czym należy zaznaczyć, iż większości ataków zapobiega się współcześnie pasywnie, stosując rozmaite środki, takie jak np. zapory ogniowe czy oprogramowanie antywirusowe. Zob. np. Trejderowski, 2013: 199.

[38] W raporcie Międzynarodowego Związku Telekomunikacyjnego wymieniono następujące cechy ułatwiające przestępczość komputerową: zbyt duże uzależnienie od technologii ICT, duża liczba użytkowników Internetu oraz technologii ICT, wysoka dostępność urządzeń tego typu oraz samego Internetu, dostępność informacji, brak mechanizmów kontroli, wielonarodowość, niezależność czasu i miejsca popełnienia przestępstwa, możliwość zautomatyzowania pewnych działań przestępczych, rosnące zdolności komputerów i przepustowość sieci, szybkość wymiany danych, szybkość rozwoju technologii, anonimowość komunikacji, brak możliwości wykorzystania tradycyjnych technik dochodzeniowych, technologie szyfrujące. Zob. *Understanding Cybercrime*…, op.cit., s. 75—84.

klasycznego systemu MAD (Mutually Assured Destruction)[39], co wynika m.in. z łatwej do osiągnięcia anonimowości atakującego bądź z braku jasnych regulacji prawnych (O'Connell, 2012). Nawet jeśli udałoby się te problemy przezwyciężyć, powstaje pytanie, na jakiej zasadzie należałoby dokonać odpowiedzi, która odstraszyłaby innych napastników. Często dokonanie kontruderzenia w sieci może być nieskuteczne bądź niemożliwe, z jednej strony wróg nie musi być bowiem uzależniony od technologii ICT (czego przykładem może być Korea Północna), z drugiej zaś w sytuacji, której źródłem ataku byłaby grupa pozapaństwowa, tego typu reakcja również byłaby niemożliwa (Berkowitz, 1997: 222—224). Na tym tle niektóre państwa, w tym np. Stany Zjednoczone, coraz częściej podkreślają możliwość konwencjonalnej odpowiedzi zbrojnej w wypadku wystąpienia poważnego cyberataku[40].

Należy ponadto podkreślić, iż cyberprzestrzeń ma jeszcze jedną cechę charakterystyczną z perspektywy bezpieczeństwa państw: otóż jest ona sferą, w której istnieje zwiększona możliwość prowadzenia działań propagandowych, co zauważyli m.in. Myriam A. Dunn (2001:145—158) czy Witold Sokała (2014: 63—73). Można przez to rozumieć również wykorzystanie technik teleinformatycznych do manipulowania opinią publiczną bądź dezinformacji. W ciekawy sposób ujęli to Agnieszka Bógdał-Brzezińska i Marcin Florian Gawrycki (2003: 94), według których

> Internet daje ogromne możliwości w komunikowaniu się i koordynowaniu akcji. W przeciwieństwie do tradycyjnych mediów jest on całkowicie niezależny od wszelkiego rodzaju grup nacisku i daje nieograniczone możliwości w propagowaniu swoich idei. Innymi słowy Internet znosi wszelkie ograniczenia, jakie wiążą się z tradycyjnymi środkami przekazu.

Wiele podmiotów cechę tę dostrzegło stosunkowo dawno. Sieć już u zarania stała się miejscem interesujących zabiegów socjotechnicznych, nakłaniania do różnorodnych postaw i wyborów ideologicznych. W ten sposób działają wbrew pozorom nie tylko sekty religijne czy fundamentaliści islamscy, ale także np. partie polityczne zatrudniające internautów do promowania ich wizji rzeczywistości społecznej i zaburzania swobodnej wymiany idei w sieci. Dość kuriozalne jest, że do tego typu działań chce uciekać się również Unia Europejska[41]. Propagandowy potencjał cyberprzestrzeni już dawno odkryli także ter-

[39] T. Shimeall, 2001, s. 16—18; *War in the Fifth Domain*. „The Economist" 01.07.2010.

[40] A. Spilius: *US could respond to cyber-attack with conventional weapons*. „The Telegraph" 01.06.2011: www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/US-could-respond-to-cyber-attack-with-conventional-weapons.html; dostęp: 12.08.2013.

[41] B. Waterfield: *EU to set up euro-election 'troll patrol' to tackle Eurosceptic surge*. „The Telegraph" 03.02.2013: www.telegraph.co.uk/news/worldnews/europe/eu/9845442/EU-to-set-up-euro-election-troll-patrol-to-tackle-Eurosceptic-surge.html; dostęp: 5.08.2013; J. Wetherell: *Spanish People's Party Hires Out Online Commenters to Toe the Party Line*. TechPresident.com,

roryści, którzy skutecznie wykorzystują ją do propagowania własnych radykalnych idei i rekrutowania zwolenników (zob. *The use of the Internet*, 2012). Przestrzeń teleinformatyczna może ponadto służyć jako skuteczny środek propagandy wojennej, co udowodniono np. w 2008 roku w czasie wojny gruzińsko-rosyjskiej, kiedy obie strony atakowały strony internetowe należące do przeciwnika, zamieszczając na nich kompromitujące materiały (Lakomy, 2010a: 185). Na tym tle działalność dezinformacyjna w sieci nawet w czasie pokoju może mieć bardzo poważne skutki dla funkcjonowania państwa. Dowodem na to stały się działania podjęte przez haktywistów w czerwcu 2011 roku, kiedy włamano się na stronę Partii Konserwatywnej w Kanadzie. Zawarto tam informacje, jakoby premier Stephen Harper znalazł się w szpitalu, co spotkało się z gwałtowną reakcją krajowych mediów[42]. Zdecydowanie poważniejszy w skutkach był atak na konto Associated Press na Twitterze w kwietniu 2013 roku. W fałszywym wpisie stwierdzono, iż w Białym Domu miały miejsce wybuchy, a prezydent Obama jest ranny, co doprowadziło to do przejściowego załamania na amerykańskiej giełdzie: indeks Dow Jones Industrial Average w ciągu ok. minuty spadł aż o 143 punkty[43]. Dowodziło to zasadniczego znaczenia działań propagandowych i dezinformacyjnych w cyberprzestrzeni dla bezpieczeństwa politycznego i gospodarczego państw, dlatego też coraz więcej rządów akcentuje zasadnicze znaczenie tego typu zagadnień. W *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space* z grudnia 2011 roku podkreślono np. możliwość prowadzenia działań psychologicznych wobec społeczeństwa rosyjskiego, którego celem byłaby jego destabilizacja lub wymuszenie na rządzie decyzji, które byłyby korzystne dla jego rywali (za: Giles, 2012: 68).

22.03.2013: http://techpresident.com/news/wegov/23644/spanish-peoples-party-hires-out-online-commenters-tow-party-line; dostęp: 5.08.2013.

[42] M. Liebowitz: *Canadian Prime Minister „Choked" in Website Attack*. Tech News Daily, 08.06.2011: www.technewsdaily.com/6895-canadian-prime-minister-choked-in-website-hack.html; dostęp: 5.08.2013.

[43] H. Moore, D. Roberts: *AP Twitter hack causes panic on Wall Street and sends Dow plunging.* „The Guardian", 23.04.2013: www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall; dostęp: 5.08.2013; P. Domm: *False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked*. CNBC, 23.04.2013: www.cnbc.com/id/100646197; dostęp: 5.08.2013.

2.4. Cyberprzestrzeń jako źródło nowych zagrożeń dla bezpieczeństwa państw

W świetle wszystkich powyższych rozważań nie dziwi fakt, iż cyberprzestrzeń zaczęła być wykorzystywana jako dogodna sfera realizacji działań uznawanych za szkodliwe z punktu widzenia bezpieczeństwa narodowego i międzynarodowego. Mogą za nimi stać podmioty o różnym statusie prawnopolitycznym, motywacjach i stopniu organizacji, począwszy od amatorów i wandali, przez wysoce wyspecjalizowanych hakerów i haktywistów, aż po organizacje terrorystyczne czy państwa (Lewis, 2012; *Communist Chinese Cyber-Attacks*). Jest więc sferą, w której zagrożenia zyskały charakter wielowymiarowy i wielopłaszczyznowy. Wyraźnie podkreślono to w amerykańskiej *Department of Defense Strategy for Operating in Cyberspace* (2011), stwierdzono tam bowiem, iż spektrum wyzwań dla bezpieczeństwa narodowego USA wykracza zdecydowanie poza wymiar militarny. Dzięki cyberatakom możliwe jest zablokowanie nie tylko systemów wojskowych, ale także elementów składających się na infrastrukturę krytyczną czy nawet naruszenie własności intelektualnej. W ciekawy sposób specyfikę tej problematyki oddał także Radosław Bania (2012: 286):

> Cyberprzestrzeń bez wątpienia wkroczyła w obręb zagadnień związanych z szeroko rozumianym pojęciem bezpieczeństwa narodowego i międzynarodowego. […] staje się obszarem, w który zostają przenoszone różnego rodzaju konflikty i który jest w szczególności otwarty na różnego rodzaju ataki, skierowane nie tylko przeciwko osobom cywilnym, ale już w znacznej mierze przeciwko istotnym elementom infrastruktury krytycznej poszczególnych państw.

Warto również zacytować słowa Tomasza R. Aleksandrowicza oraz Krzysztofa Liedela (2014: 11), według których

> nowym środowiskiem walki stała się cyberprzestrzeń, będąca areną działań o charakterze wojskowym (ataki na systemy dowodzenia i łączności przeciwnika) i wywiadowczym, sabotażowym czy wręcz przestępczym (np. kradzieże komputerowe), a nawet chuligańskim, nie wspominając o działaniach propagandowych czy politycznych. Stwarza to nowe zagrożenia dla bezpieczeństwa narodowego, bowiem w coraz większym stopniu elementy infrastruktury krytycznej państw funkcjonują w oparciu o technologie informacyjne i są podatne na zagrożenia z cyberprzestrzeni.

Na tym tle warto prześledzić ewolucję wyzwań dla bezpieczeństwa teleinformatycznego państw. W ujęciu historycznym pierwsze akty łamania zabezpieczeń komputerowych miały miejsce jeszcze przed powstaniem ARPANET-u.

Proceder ten upowszechnił się jednak dopiero w latach 70. i 80. XX wieku wraz z popularyzacją komputerów osobistych (Clarke, Clawson, Cordell, 2003). Towarzyszyło temu zjawisko powstawania pierwszych typów złośliwego oprogramowania. Domorośli specjaliści łamali nieliczne i mało wówczas zaawansowane zabezpieczenia ośrodków naukowych, korporacji i administracji państwowej, zarówno dla własnej satysfakcji, pryncypiów ideologicznych, jak i dla określonych korzyści materialnych. Już w 1987 roku grupa VAXBusters włamała się do serwerów NASA oraz komputerów znajdujących się w amerykańskiej bazie wojskowej w Rammstein. Często w tym kontekście wspomina się również o działalności Markusa Hessa, niemieckiego hakera odpowiedzialnego za włamania do Pentagonu oraz Massachussetts Institute of Technology. Tym, co go wyróżniało, był fakt, iż był on opłacany przez kraje bloku komunistycznego[44]. Źródła dotyczące szkodliwej działalności w cyberprzestrzeni często wspominają także o pierwszym, choć niepotwierdzonym akcie cyberterroryzmu państwowego: według niektórych informacji w 1982 roku Centralna Agencja Wywiadowcza USA (CIA) zainstalowała w kanadyjskim programie przemysłowym tzw. bombę logiczną. Program ten miał zostać później wykradziony przez radzieckich szpiegów, którzy użyli go w systemie zarządzającym rurociągami na Syberii, co w efekcie miało doprowadzić do ogromnej eksplozji (*War in the Fifth Domain*, 2010; Clarke, Knake, 2010: 93). Wydarzenia te nie zostały jednak nigdy w pełni potwierdzone.

Z dzisiejszej perspektywy wszystkie ówczesne przedsięwzięcia miały bardzo ograniczoną skalę. Państwa, które stawiały wówczas pierwsze kroki w tej dziedzinie, traktowały te działania głównie jako eksperyment, a nie poważną inicjatywę (Łapczyński, 2009), choć warto pamiętać, iż w wymiarze deklaratywnym już wówczas podkreślano istotne znaczenie tych zagadnień. Świadczyło o tym np. stanowisko Ronalda Reagana z 1984 roku, który w *National Security Devision Directive* 145 stwierdził: „technologia wykorzystywania systemów elektronicznych jest powszechna i wykorzystywana przez obce narody oraz może być zastosowana również przez grupy terrorystyczne i element przestępczy" (Dunn-Cavelty, 2008: 61).

Znaczenie cyberprzestrzeni jako źródła nowych wyzwań dla bezpieczeństwa państw zaczęło rosnąć dopiero w latach 90. XX wieku, wraz z postępem rewolucji informatycznej. Świadczył o tym gwałtowny rozwój złośliwego oprogramowania, które mimo niewielkiego zasięgu Internetu było w stanie szybko rozprzestrzeniać się po całym globie. Już w 1992 roku światową akcję prewencyjną wywołał wirus *Michelangelo*, który według pierwszych raportów miał zainfekować ok. 5 milionów komputerów. Dzięki ostrzeżeniom mediów w rzeczywistości liczbę tę udało się zredukować do kilku tysięcy. Podobną inicja-

[44] T. Formicki: *Komandosi cyberprzestrzeni*. „Stosunki Międzynarodowe" 07.11.2007: www.stosunki.pl/?q=node/1106; dostęp: 7.08.2013.

tywę kilka lat później wywołał wirus *Boza*[45]. W 1999 roku światowy rozgłos zyskał również wirus *Melissa*, który w odróżnieniu od swoich poprzedników rzeczywiście doprowadził do poważnych strat finansowych, ocenianych na ok. 1 miliard dolarów. Jego cechą szczególną był fakt, iż wykorzystywał do rozprzestrzeniania się prężnie wówczas rozwijający się Internet. Jeszcze większe straty, szacowane na 5,5 do 8,7 mld dolarów, przyniósł wykorzystujący mechanizmy inżynierii społecznej wirus *I love you* (Lakomy, 2011a: 142—143). Świadczyło to o znaczącym postępie w zakresie skuteczności nowych typów złośliwego oprogramowania. Na początku lat 90. XX wieku były to głównie ciekawe, lecz stosunkowo mało skomplikowane wirusy, z czasem jednak pojawiły się nowe ich formy, w tym np. wersje polimorficzne[46] (*One Half* z 1994 roku), które później wyewoluowały w oprogramowanie metamorficzne[47]. Ponadto zaczęły się rozprzestrzeniać pierwsze robaki komputerowe (np. *Happy99* z 1999 roku, *Blaster/Lovesan* z 2003 roku, *Netsky* z 2004 roku) czy trojany (*Graybird* z 2003 roku). Na przełomie wieków głównym nośnikiem *malware* stała się poczta elektroniczna, która nie tylko umożliwiała błyskawiczną transmisję programu, ale też wykorzystanie inżynierii społecznej. Później rolę tę przejęły inne usługi i aplikacje, takie jak np. media społecznościowe. Przykładem był tu rozprzestrzeniający się w latach 2008—2009 robak *Koobface*, atakujący użytkowników Facebooka i Myspace[48]. Warto dodać, iż w 2009 roku nowy wariant złośliwego oprogramowania pojawiał się w sieci średnio co 2,2 sekundy (Clarke, Knake, 2010: 89).

Procesom tym towarzyszyło powstawanie nowych form szkodliwej działalności w sieci. Przede wszystkim doszło do lawinowego zwiększenia skali różnorodnie motywowanych cyberataków. Część z nich wynikała z chęci sprawdzenia indywidualnych umiejętności programistycznych, inne były związane z określonymi postawami ideologicznymi, religijnymi, politycznymi bądź działalnością *stricte* kryminalną. Pojawiły się wreszcie pierwsze przypadki poważnego naruszenia bezpieczeństwa państw. Warto scharakteryzować pokrótce kilka wybranych przejawów tych tendencji:

---

[45] M. Byrne: *How the Michalangelo Virus Infected Us and the World Learned the Name „McAfee"*. Motherboard: http://motherboard.vice.com/blog/how-the-michelangelo-virus-infected-us-and-the-world-learned-the-name-mcafee; dostęp: 7.08.2013; *Boza.A*. F-Secure: www.f-secure.com/v-descs/boza.shtml: dostęp: 7.08.2013.

[46] Według Macieja Miłostana z Politechniki Poznańskiej jest to „stały kod wirusa, zaszyfrowany zmienną procedurą szyfrującą". Za: M. Miłostan: *Ochrona danych i kryptografia. Wirusy i robaki*. Politechnika Poznańska, s. 7: www.cs.put.poznan.pl/mmilostan/zaoczne/SUM/Wirusy.pdf; dostęp: 12.08.2014.

[47] Charakteryzuje się on tym, iż „cały kod wirusa jest modyfikowany, zmienia się rozmieszczenie bloków instrukcji, różne ciągi instrukcji o tym samym działaniu". Za: M. Miłostan, op.cit.

[48] Zob. np. T. Grudziecki: *Cyberataki wczoraj, dziś i jutro*. CERT Polska: www.nask.pl/files/p/Cyberataki_wczoraj_dzis_i_jutro.pdf; dostęp: 7.08.2013.

1. Już w 1997 roku Stany Zjednoczone rozpoczęły wewnętrzne ćwiczenia z zakresu cyberbezpieczeństwa o kryptonimie *Eligible Receiver*. Polegały one na wydzieleniu specjalnej grupy hakerów pracujących dla NSA, których zadaniem było włamanie się m.in. do systemów teleinformatycznych Pentagonu. Wbrew oczekiwaniom grupa ta osiągnęła znaczne sukcesy, uzyskując dostęp m.in. do komputerów dowództwa United States Pacific Command, sieci elektroenergetycznych i linii alarmowych 911. Według ówczesnego zastępcy sekretarza obrony USA Johna Hamre'a ćwiczenia te zademonstrowały kompletny brak świadomości zagrożeń dla bezpieczeństwa teleinformatycznego[49].
2. Opinię tę potwierdziła seria trwających od marca 1998 roku włamań do serwerów należących do Pentagonu, NASA, Departamentu Energii oraz amerykańskich uniwersytetów i ośrodków badawczych. W ich wyniku wyprowadzono z serwerów dziesiątki tysięcy plików dotyczących instalacji militarnych, rozmieszczenia wojsk, szyfrów czy technologii wojskowych. Źródłem ataku był komputer znajdujący się na terenie jednego z państw byłego Związku Radzieckiego. Rosja odżegnała się jednak od odpowiedzialności za te incydenty, które określono mianem *Moonlight Maze*[50]. Rezultatem ujawnienia tej sprawy stało się większe zainteresowanie rządu USA problematyką cyberbezpieczeństwa.
3. Pod koniec lat 90. XX wieku wystąpiły poważne incydenty w Azji Południowo-Wschodniej. Aby wywrzeć nacisk na władze Indonezji w sprawie Timoru Wschodniego, haktywiści zagrozili, iż sparaliżują system bankowy tego kraju. Z kolei w latach 1999—2000 doszło do ponad setki włamań na witryny internetowe należące do rządu Malezji (Moćkun, 2009: 2; Łapczyński, 2009: 1; Sienkiewicz, 2003: 376—377, za: Lakomy, 2011a: 143).
4. Przestrzeń teleinformatyczna stała się areną zmagań podczas wojny w Kosowie w 1999 roku. Serbscy hakerzy wykorzystali sieć, aby zaatakować strony internetowe bombardującego ich kraj Sojuszu Północnoatlantyckiego. Te same działania podjęli również programiści chińscy po zniszczeniu przez Pakt ambasady ChRL w Belgradzie. Jednym z najważniejszych efektów tych wydarzeń było większe zainteresowanie tematyką bezpieczeństwa teleinformatycznego przez NATO[51].
5. O lawinowym wzroście cyberzagrożeń na przełomie XX i XXI wieku świadczyła także afera, która wybuchła w lecie 2001 roku w USA. Doszło

[49] Hildreth, 2002: 5; *The Warnings?* Public Broadcasting Service: www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings; dostęp: 8.08.2013.

[50] *We're in the Middle of a Cyber War.* „The Daily Beast", 19.09.1998: www.thedailybeast.com/newsweek/1999/09/19/we-re-in-the-middle-of-a-cyerwar.html; dostęp: 8.08.2013.

[51] Borger, 1999; J. Carr: *Real Cyber Warfare: Carr's Top Five Picks*. Forbes, 02.04.2011: www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks; dostęp: 8.08.2013; Dunn-Cavelty, 2008: 73—75.

wówczas do serii włamań do komputerów miasta Mountain View w Kalifornii. Poszukiwano w ten sposób informacji dotyczących m.in. świadczonych przez ratusz usług, systemów alarmowych czy biur rządowych. FBI odkryło, iż komputery, z których dokonano ataków, znajdowały się na Bliskim Wschodzie, z czego wysnuto tezę o możliwym zagrożeniu terrorystycznym. Po zamachach na World Trade Center opinia ta została potwierdzona, na przejętych komputerach Al Kaidy odkryto bowiem wykradzione materiały na ten temat. Richard Clarke, ówczesny doradca prezydenta Stanów Zjednoczonych ds. cyberbezpieczeństwa, zauważył w tym kontekście, iż sprawa ta udowodniła, jak łatwo można z zagranicy uzyskać dane dotyczące fizycznej i cyberprzestrzennej infrastruktury USA[52].

W kolejnych latach powyższe tendencje przybrały jedynie na sile, oprócz kryminalistów, hakerów i haktywistów na stałe domeną tą zainteresowały się bowiem bardziej zorganizowane podmioty. Z jednej strony dotyczyło to organizacji terrorystycznych oraz innych radykalnych grup politycznych i religijnych, z drugiej natomiast państw i ich organizacji (np. NATO). W związku z tym skala zagrożeń teleinformatycznych zyskała wcześniej niespotykany poziom. Za przełom w tym zakresie uznaje się wydarzenia w Estonii, która jako pierwsza w historii została na masową skalę zaatakowana przez Internet w kwietniu 2007 roku. Niedługo później technologie teleinformatyczne odegrały istotną rolę w izraelskiej operacji zbrojnej przeciwko Syrii oraz w wojnie gruzińsko-rosyjskiej. Każdy z tych incydentów udowodnił, jak wielki potencjał dla realizacji określonych interesów w środowisku międzynarodowym posiada cyberprzestrzeń, zarówno w czasie pokoju, jak i podczas konfliktu zbrojnego. Doprowadziło to w efekcie również do popularyzacji terminu *cyberwojny* (Lakomy, 2010b: 61—62).

Skalę wyzwań, które pojawiły się w pierwszej dekadzie XXI wieku, najlepiej obrazują statystyki. Już w 2003 roku straty finansowe wynikające z przestępczości komputerowej oceniano na sumę ok. 17 mld dolarów. Tymczasem w cztery lata później dochody z tego procederu przekroczyły zyski z globalnego handlu narkotykami. W 2007 roku oceniano, iż cyberprzestępczość pozwoliła różnorodnym podmiotom zarobić w ciągu dwunastu miesięcy ok. 100 mld dolarów (*Understanding Cybercrime*, 2012: 2). W związku z tym w Internecie zaczęło się rozprzestrzeniać specjalnie zaprojektowane złośliwe oprogramowanie, którego celem stał się wyłącznie sektor finansowy. Przykładem był tu np. robak *Nimda*, który pojawił się online 18 września 2001 roku[53]. Rosnącym stratom finansowym sprzyjała coraz większa liczba incydentów teleinformatycz-

[52] *The Warnings?* Public Broadcasting Service: www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings; dostęp: 8.08.2013.

[53] P. Wood: *Nimda — the worm finds new tricks*. Symantec: www.symantec.com/connect/blogs/nimda-worm-finds-new-tricks; dostęp: 8.08.2013.

nych. W 2008 roku komputery Departamentu Stanu USA były atakowane ok. 6 milionów razy każdego dnia, co oznaczało wzrost w stosunku do 2007 roku aż o 46% (Coleman, 2008: 4). Jednym z powodów tego stanu rzeczy było pojawienie się pierwszych masowych sieci *botnet*[54]. W 2007 roku tylko jedna sieć komputerów *zombie*[55] w USA, która była kontrolowana przez chińskich przestępców, oceniana była na ok. 730 000 jednostek. W rok później globalny *botnet* o kryptonimie *Storm* obejmował zawrotną liczbę od 20 do 115 milionów komputerów[56].

Mimo że cyberbezpieczeństwo stało się jednym z najczęściej omawianych wyzwań globalnych, na początku drugiej dekady XXI wieku problemy te uległy jedynie dalszemu pogłębieniu. Świadczyły o tym informacje zawarte w *Norton Cybercrime Report* z 2012 roku, który objął badaniem 24 państwa. Według jego autorów straty finansowe wynikające jedynie z wykrytej cyberprzestępczości wynosiły ok. 110 mld dolarów rocznie. Każdego dnia ofiarą ataków w przestrzeni teleinformatycznej padało wówczas ok. 1,5 mln użytkowników, co dawało zawrotną liczbę 556 mln rocznie (18 osób co sekundę). Według danych Symantec aż 2/3 dorosłych korzystających z Internetu padło ofiarami przestępstwa komputerowego. Raport wskazywał, że szkodliwa działalność w sieci coraz częściej dotyczyła urządzeń mobilnych, takich jak np. smartfony czy tablety (*2012 Norton Cybercrime Report*, 2012; Łapczyński, 2009: 1; Brągoszewski, 2007). Statystyki te, jakkolwiek mające charakter orientacyjny i wycinkowy, oddawały skalę zagrożeń, które pojawiły się w wyniku rewolucji informatycznej, stało się bowiem jasne, iż w przeciwieństwie do tradycyjnej formy przestępczości czy działań terrorystycznych ataki w sieci zaczęły dotyczyć większości internautów.

Na tym tle warto więc przywołać najbardziej aktualne statystyki i dane z roku 2013. Przede wszystkim należy podkreślić, iż stale zwiększała się liczba cyberataków, choć zmieniały się ich główne cele. Do najczęstszych zaliczono system Android, właściwy urządzeniom przenośnym, takim jak tablety bądź

---

[54] Rozumie się przez to grupę komputerów zainfekowanych złośliwym oprogramowaniem i kontrolowanych z ukrycia przez hakerów zarządzających daną siecią, które mogą być następnie wykorzystywane np. do rozsyłania spamu, cyberataków typu DDoS czy innych szkodliwych działań online. Zob. Mehan, 2008: 60; B. Łącki: *Botnet od podszewki*. „Heise Security" 13.06.2007: www.heise-online.pl/security/features; dostęp: 6.08.2013; Thonnard, Mees, Dacier, 2009; Leder, Werner, Martini, 2009; Czosseck, Klein, Leder, 2011.

[55] To komputery, które bez zgody i wiedzy właściciela są kontrolowane z zewnątrz za pomocą złośliwego oprogramowania. Wchodzą w skład *botnetów* i mogą zostać wykorzystane np. do ataków DDoS lub rozsyłania spamu. Zob. *Terms & Definitions of Interest for DoD Counterintelligence Professionals*. Defense Intelligence Agency, 02.05.2011, s. 182: http://fas.org/irp/eprint/ci-glossary.pdf; dostęp: 12.08.2014; Harley, Lee, Borghello, 2009, s. 5.

[56] *Cyber Crime Statistics and Trends*. GO-Gulf.com: www.go-gulf.com/blog/cyber-crime; dostęp: 8.08.2013.

smartfony. Innym obiektem zainteresowania cyberprzestępców stały się media społecznościowe. Na najpopularniejszym portalu tego typu — Facebooku — cyberprzestępcy włamywali się na ok. 600 000 kont dziennie, a zatem średnio co dziesiąty użytkownik tego typu serwisów utracił w ten sposób prywatne dane. Ciekawym i coraz bardziej rozpowszechnionym zjawiskiem stało się również *ransomware*, polegające na zainfekowaniu komputera szkodliwym kodem i zażądaniu okupu w zamian za jego usunięcie. Co prawda jego źródeł można się upatrywać jeszcze w latach 80. XX wieku, jednak dopiero na początku drugiej dekady XXI wieku stało się ono powszechne. Stale wzrastała również liczba zainfekowanych stron WWW: w 2011 roku było ich ok. 55 000, podczas gdy rok później już 74 000. Coraz częściej podejmowano także próby włamań do serwerów wojskowych, np. komputery US Navy w ciągu godziny były atakowane w cyberprzestrzeni ok. 110 000 razy[57]. Wbrew pozorom nie są to jednak najczęstsze cele ataków. Zagadnienie to obrazuje Tabela 1.

Tabela 1

Podział włamań komputerowych ze względu na ich cele

Sektor	Ataki [%]	Sektor	Ataki [%]
Przemysł	24	Usługi profesjonalne	8
Finanse, ubezpieczenia, rynek nieruchomości	19	Przemysł kosmiczny	2
Usługi nietradycyjne	17	Handel detaliczny	2
Rząd	12	Handel hurtowy	2
Energia	10	Transport, komunikacja, dostawy gazu	1

Źródło: opracowanie własne na podstawie: *Internet Security Threat Report 2013*. Symantec. T. 18, s. 15.

Powyższe dane świadczą o tym, iż najczęstszym obiektem ataków pozostawał sektor prywatny, w tym głównie przedsiębiorstwa. Podstawowym powodem szkodliwej działalności były zatem pobudki kryminalne, związane z uzyskaniem określonych korzyści materialnych. Jednocześnie bardzo duży procent włamań obejmował obszary o żywotnym znaczeniu dla bezpieczeństwa państw, wchodzące w skład infrastruktury krytycznej.

Na tej podstawie warto jeszcze prześledzić, jakie w tym czasie były źródła najpoważniejszych zagrożeń bezpieczeństwa teleinformatycznego. Wbrew pozorom nie były one tak oczywiste, jak mogłoby się wydawać, biorąc pod uwagę

[57] *Internet Security, 2013; Cyber Crime Statistics and Trends*. GO-Gulf.com: www.go-gulf.com/blog/cyber-crime; dostęp: 8.08.2013.

chociażby fakt, iż do największych producentów szkodliwego oprogramowania na świecie, obok Federacji Rosyjskiej, zalicza się z reguły Stany Zjednoczone[58]. Z tego typu informacjami jest jednak pewien problem, ponieważ równolegle pojawiają się statystyki, które częstokroć prezentują zupełnie odmienne dane, przygotowane w oparciu o inną metodologię badań. Obrazują to poniższe tabele.

Tabela 2

Źródła ataków według Europolu
(stan na 2010 rok)

Państwo	Cyberataki [%]	Państwo	Cyberataki [%]
Stany Zjednoczone	23	Hiszpania	4
Chiny	9	Włochy	3
Niemcy	6	Francja	3
Wielka Brytania	5	Turcja	3
Brazylia	4	Polska	3

Źródło: opracowanie własne na podstawie: *Europol: The Center to Fight Cybercrime*. 2010: www.intellectualtakeout.org/library/chart-graph/countries-cyber-attack; dostęp: 8.08.2013.

Tabela 3

Źródła ataków według
2013 Data Breach Investigations Report

Państwo	Cyberataki [%]	Państwo	Cyberataki [%]
Chiny	30	Holandia	1
Rumunia	28	Armenia	1
Stany Zjednoczone	18	Niemcy	1
Bułgaria	7	Kolumbia	1
Rosja	5	Brazylia	1

Źródło: opracowanie własne na podstawie: *2013 Data Breach Investigations Report*. Verizon RISK Team 2013, s. 22.

[58] Ibidem.

Tabela 4

Źródła cyberataków według raportu *State of the Internet* (stan na początek 2013 roku)

Państwo	Cyberataki [%]	Państwo	Cyberataki [%]
Chiny	34,0	Indie	2,6
Rumunia	21,0	Tajwan	2,5
Stany Zjednoczone	8,3	Brazylia	2,2
Turcja	4,5	Rumunia	2,0
Rosja	2,7	Hong Kong	1,6

Źródło: opracowanie własne na podstawie: *State of the Internet*. Akamai 2013. Zob. *China, Indonesia lead sources of online attacks: Study*. „The Express Tribune" 24.07.2013: http://tribune.com.pk/story/581189/china-indonesia-lead-sources-of-online-attacks--study; dostęp: 8.08.2013; *Akamai's study says Indonesia is 2nd largest source of cyber attacks*. E27, 24.07.2013: http://e27.co/2013/07/24/indonesia-rises-to-2nd-place-in-akamais-latest-study-on-cyber-attacks; dostęp: 8.08.2013.

Powyższe dane, jakkolwiek dość różnorodne, dają jednak pewne pojęcie o najpoważniejszych źródłach ataków w przestrzeni teleinformatycznej: od lat do państw najbardziej aktywnych w tej dziedzinie zalicza się bowiem Stany Zjednoczone, Chiny oraz Rosję.

Ze względu na wszystkie omówione wyżej procesy nie dziwi fakt, iż przestrzeń teleinformatyczna nie tylko zaczęła być wyodrębniana jako osobny wymiar bezpieczeństwa państw, lecz także jako kolejny, piąty teatr wojny, obok lądu, powietrza, morza oraz przestrzeni kosmicznej. Jean Guisnel (1997a: 209) przyrównał ją wręcz do nowego „wielkiego pola manewrów". W XXI wieku coraz więcej armii zaczęło uświadamiać sobie znaczenie zdobywania, przetwarzania i transmisji informacji na polu walki za pomocą systemów i sieci teleinformatycznych. Przemiany te z reguły określa się mianem RMA (Revolution in Military Affairs[59]), rewolucji, która obejmuje swoim zasięgiem m.in. powstanie wspomnianej już koncepcji sieciocentrycznego pola walki, koncepcji zintegrowanej walki (*integrated warfare*), wykorzystywanie systemów AWACS (Airborne Early Warning and Control System), wykorzystanie aparatów bezzałogowych (np. dronów) czy inteligentnego, precyzyjnego uzbrojenia (Saalbach, 2013: 6—7). Za symbol RMA, a więc za przejaw wyodrębnienia cyberprzestrzeni jako kolejnego teatru wojny, należy z pewnością uznać koncepcję sieciocentrycznego pola walki (Network-Centric Warfare), którą po raz pierwszy zaproponował wiceadmirał amerykańskiej armii Arthur C. Cebrowski. Nie ma jednoznacznej definicji tego pojęcia, lecz najogólniej rzecz biorąc, sieciocentryczne pole walki polega na efektywnym wykorzystaniu osiągnięć informatyki

[59] Zob. Murray, 1997; Mazarr, 1994; Sullivan, Coroalles, 1995; Sharma, 2009; Dunn-Cavelty, 2002: 102—121; Delpech, 2001; Bédar, 2001.

na wszystkich szczeblach dowodzenia dla osiągnięcia zwiększonej skuteczności w walce. Współcześnie siły zbrojne wielu państw starają się wdrożyć nowe technologie do działań na lądzie, morzu i w powietrzu. W niedalekiej przyszłości rozmaite programy „żołnierza przyszłości" (np. projekt „Tytan" Polskiego Holdingu Obronnego) wplotą najnowsze technologie ICT w działania nawet pojedynczych żołnierzy. Nie chodzi tu jedynie o rzecz fundamentalną dla skuteczności działań zbrojnych, czyli utrzymanie łączności, sieciocentryczność kładzie bowiem nacisk nie tylko na jej skuteczność, ale także skalę, szybkość, zwiększoną możliwość koordynacji poszczególnych oddziałów czy bardziej efektywne rozpoznanie, m.in. dzięki możliwości bezpośredniego śledzenia działań żołnierzy na polu walki. Rewolucja informatyczna dała wojsku narzędzia niezbędne do tego, aby skutecznie sprząc wszystkie składające się na nie elementy w jeden sprawnie działający organizm[60]. Powstawaniu nowych wyzwań dla bezpieczeństwa w cyberprzestrzeni towarzyszy zatem proces swoistego „zanurzania się" sił zbrojnych w tej domenie, z czym wiążą się zarówno oczywiste korzyści, jak i kolejne wyzwania.

Należy jednak podkreślić, iż w takim ujęciu jest to sfera jakościowo odmienna od pozostałych teatrów działań zbrojnych, co wynika z dwóch powodów. Przede wszystkim, jak zauważył Nils Melzer (2011: 5), jest to jedyna domena, która została w całości stworzona przez człowieka, po drugie natomiast manipulacja danymi w formie cyfrowej może dotyczyć zarówno infrastruktury czy urządzeń znajdujących się na ziemi, samolotów, okrętów wojennych, jak i satelitów zlokalizowanych w przestrzeni kosmicznej (Kallberg, 2012: 124—134; Creedon, 2012: 3—8). Będąc osobnym teatrem działań zbrojnych, w zasadzie przenika ona wszystkie pozostałe.

Współcześnie procesy te zostały prawidłowo dostrzeżone przez większość państw świata. Już w 2007 roku aż 120 z nich prowadziło prace zmierzające do uzupełnienia swojego potencjału militarnego o komponent cyberprzestrzenny (Melnitzky, 2012: 542). Na tym tle pojawiło się wręcz pojęcie *cyberpotęgi*, którą można zdefiniować jako „zdolność do wykorzystania cyberprzestrzeni do uzyskania korzyści lub wpływu na wydarzenia we wszystkich środowiskach operacyjnych" (Kuehl, 2009: 37—38). Dan Kuehl przyrównał ją również do potęgi morskiej, przez którą rozumiało się zdolność narodu do narzucenia swojej woli na morzu (Ibidem, s. 37—38; szerzej na ten temat: Huber, 1997: 191—195).

Ogólnie rzecz biorąc, sfera ta przekracza więc tradycyjne granice, nie tylko jeśli chodzi o płaszczyznę fizyczną (Bendiek, 2012: 6). Najpełniej kwestię tę uchwycili Roger C. Molander, Peter A. Wilson i Andrew S. Riddile (1996: 22).

---

[60] Zob. Alberts, Garstka, Stein, 1999: 6—7; Szubrycht, 2004: 143—154; Bogdański, 2012: 68—69; Gulbas, 2012: 6—9; *Polski żołnierz przyszłości*. Polski Holding Obronny: www.pho.pl/oferta/projekty-strategiczne/polski-zolnierz-przyszlosci; dostęp: 7.08.2013; Metz, 2000: 56—61.

Ich zdaniem ten nowy wymiar bezpieczeństwa wiąże się z zaburzeniem konwencjonalnego podziału między wojną i pokojem, wojną a przestępstwem, polityką wewnętrzną i zagraniczną, sektorem prywatnym i publicznym, sprawami wojskowymi i komercyjnymi oraz wyzwaniami strategicznymi i taktycznymi. Według autorów z powodu specyfiki przestrzeni teleinformatycznej rosnące wątpliwości dotyczą także administracyjnego podziału obowiązków, określonej jurysdykcji czy wreszcie obowiązujących koncepcji bezpieczeństwa. Nie zawsze zatem wiadomo „kto jest atakowany, przez kogo… oraz kto dowodzi" (Ibidem).

Pojawiające się w cyberprzestrzeni zagrożenia ze względu na swój charakter przenikają wszystkie instytucje i mechanizmy państwowe, wymuszając wprowadzenie niezbędnych zmian. Całość tych procesów trafnie scharakteryzowali Piotr Sienkiewicz i Halina Świeboda (2009: 77—78). Ich zdaniem

> od powstania Internetu szczególne znaczenie zyskał technologiczny wymiar globalizacji, związany z wysoką dynamiką zmian w sferze komunikacji i informacji, a także postępującą integracją systemów informatycznych i telekomunikacyjnych. Pogłębiło to charakter zjawisk składających się na globalizację, przenosząc pewne procesy gospodarcze, społeczno-polityczne i kulturowe w przestrzeń wirtualną. […] W wyniku tych oraz innych procesów powstała „przestrzeń cybernetyczna" (*cyberspace*), nieskrępowana czasem i odległością, której granice wyznacza jedynie aktualny poziom rozwoju techniki informacyjno-komunikacyjnej. […] Wraz z postępem technologicznym i rozwojem Internetu narodziły się jednak nowe zagrożenia, którym towarzyszyła kumulacja i transformacja już istniejących. Pojawiły się również nowe obszary bezpieczeństwa informacyjnego, które w przeszłości były kojarzone z wąsko rozumianą ochroną informacji objętych tajemnicą państwową i służbową. Niegdyś w sferze zagrożeń bezpieczeństwa państwa dominowały takie zjawiska, jak szpiegostwo, działalność dywersyjna, przekazywanie informacji nieuprawnionym podmiotom itp. Poprzez rozwój technik ICT uzyskały one nową jakość i stały się groźniejsze dla bezpieczeństwa narodowego. Wraz z rozwojem technologicznym nasiliła się też konieczność zapewnienia systemom i sieciom informacyjnym stabilności działania, poufności, integralności i nienaruszalności.

Reasumując ten wątek, należy więc podkreślić, iż cyberprzestrzeń dzięki swoim unikalnym właściwościom stała się od przełomu XX i XXI wieku sferą, w której pojawiły się nowe zagrożenia bezpieczeństwa narodowego i międzynarodowego. Można zgodzić się z Kennethem Geersem (2014: 11), który stwierdził, że Internet miał w założeniu przyczynić się do bardziej pokojowej przyszłości całej ludzkości, współcześnie stosunki międzynarodowe w cyberprzestrzeni bliższe są jednak kategorii „pandemonium niż raju". Zagrożenia teleinformatyczne, mając dynamiczny, wielowymiarowy i wielopłaszczyznowy charakter, przyjmują zróżnicowane formy, uzależnione zresztą od przyjętej optyki

badawczej. W sieci działają nie tylko różnorodnie motywowane jednostki, ale także pewne nieformalne grupy (organizacje przestępcze czy terrorystyczne), a nawet same państwa (zob. Billo, Chang, 2004). Te ostatnie dzięki wskazanym wyżej cechom przestrzeni teleinformatycznej w coraz większym stopniu zaczęły dostrzegać znaczenie tej domeny. Chodzi tu nie tylko o zapewnienie korzyści politycznych, gospodarczych czy społecznych wynikających z prawidłowego funkcjonowania infrastruktury teleinformatycznej, część rządów zaczęła bowiem odczuwać nie tylko potrzebę zwalczania pojawiających się tam zagrożeń, ale wręcz wykorzystania jej najważniejszych cech dla realizacji określonych interesów w środowisku międzynarodowym. Wszystkie omówione wcześniej właściwości cyberprzestrzeni, jak również występujące tam w ostatnich dekadach tendencje, paradoksalnie sprzyjają tego typu nowatorskiej aktywności.

Rozdział 3

Formy zagrożeń teleinformatycznych dla bezpieczeństwa państw

3.1. Zagrożenia w cyberprzestrzeni w ujęciu podmiotowym

Zagrożenia dla bezpieczeństwa można zdefiniować jako

> taki splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do nie zakłócanego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych — w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp. (Nowak, Nowak, 2011: 40).

Zrozumienie istoty wykorzystania cyberprzestrzeni przez państwa w celu realizacji określonych interesów w środowisku międzynarodowym powinno być poprzedzone pogłębioną analizą samych zagrożeń w tej dziedzinie. Wynika to z dwóch powodów. Przede wszystkim rywalizacja rządów w tej domenie wpisuje się w szerszy obraz problemów bezpieczeństwa teleinformatycznego. Cyberataki inspirowane bądź przeprowadzane przez siły zbrojne i wyspecjalizowane agencje są z pewnością jedną z najgroźniejszych, lecz nie jedyną formą wyzwań w sieci. Badanie tych zagadnień powinno zatem wziąć pod uwagę naturę innych zagrożeń pojawiających się w cyberprzestrzeni, chociażby ze względu na trudności interpretacji poszczególnych incydentów czy na potrzebę stosowania sprecyzowanej nomenklatury naukowej. Po drugie charakter tych problemów jest jednym z głównych determinantów aktywności państw w przestrzeni teleinformatycznej. Z jednej strony wpływa na ich rywalizację, wyspec-

jalizowane struktury rządowe uczą się bowiem nowych technik i metod włamań, opracowują nowe środki ataków w dynamicznym środowisku, złożonym w głównej mierze z podmiotów nisko zorganizowanych, pozapaństwowych. W tym kontekście dochodzi więc do swoistego sprzężenia zwrotnego między różnymi aktorami funkcjonującymi w przestrzeni teleinformatycznej. Rodzaje cyberataków, ich skuteczność, sposób zorganizowania, obrane cele oraz wynikające z nich konsekwencje są wyjątkowym materiałem poglądowym, który determinuje działania podejmowane przez agencje rządowe nie tylko w wymiarze defensywnym, ale także ofensywnym. Z drugiej strony zagrożenia bezpieczeństwa teleinformatycznego stanowią podstawowy czynnik warunkujący międzynarodową współpracę w tej dziedzinie. Główną motywacją, która stoi za inicjatywami w tym zakresie, jest właśnie bogactwo i dynamika wyzwań dla cyberbezpieczeństwa, które pojawiły się w ciągu ostatnich trzech dekad. Ich charakterystyka wydaje się warunkiem *sine qua non* realizacji postawionego we wstępie celu badawczego.

Tego typu przedsięwzięcie napotyka jednak szereg podstawowych problemów, związanych głównie z wielowymiarowością, wielopłaszczyznowością czy płynnością tych zjawisk. Marek Madej i Marcin Terlikowski (2009: 9) słusznie stwierdzili, iż wynika to z różnorodności i dużej liczby poziomów, na których należy rozpatrywać bezpieczeństwo teleinformatyczne:

> począwszy od użytkownika indywidualnego (poziom najniższy) — przeciętnego obywatela posługującego się komputerem osobistym — przez przedsiębiorstwa i instytucje, wykorzystujące w swej codziennej działalności całe sieci teleinformatyczne, aż po samo państwo (jego struktury administracyjne, organy i służby czy też gospodarkę).

Formy zagrożeń teleinformatycznych różnią się zdecydowanie, jeśli weźmie się pod uwagę np. stosowane metody w ujęciu nauk technicznych, motywacje sprawców, stopień organizacji bądź ich status prawnomiędzynarodowy. W każdym wypadku wynik analizy będzie odmienny, co też rodzi zasadniczą trudność z punktu widzenia prowadzonych badań. Sytuację dodatkowo komplikuje fakt, iż cyberataki mogą mieć bardzo różnorodne konsekwencje, zarówno w wymiarze *stricte* technicznym, prawnym, politycznym, gospodarczym, jak i społecznym. Za przykład mogą służyć wydarzenia w Estonii w 2007 roku, które miały z punktu widzenia bezpieczeństwa państwa zupełnie odmienny charakter niż np. działalność chińskiej siatki szpiegowskiej *Gh0stnet*. Podobną analogię można odnaleźć, porównując np. regularne włamania komputerowe przeprowadzane przez pospolitych przestępców oraz aktywność grup terrorystycznych (Terlikowski, 2009: 120; Lakomy, 2013d). Znalezienie więc rozwiązania, które pozwoliłoby uchwycić zarówno charakter samych zagrożeń, jak i istotne dla nauk politycznych konsekwencje, wydaje się zadaniem niezwykle trudnym.

Z perspektywy omawianego tematu badawczego wydaje się, iż charakterystykę tych zagadnień należałoby rozpocząć od kwestii podstawowej, czyli podmiotów podejmujących szkodliwe działania w cyberprzestrzeni. Jest to zadanie stosunkowo trudne, biorąc pod uwagę liczbę użytkowników samego tylko Internetu oraz mnogość wejść do systemu. Sytuację dodatkowo komplikuje fakt, iż należałoby rozpatrzyć nie tylko pojedynczych użytkowników, ale także różnorodne struktury społeczne i polityczne funkcjonujące w tej domenie oraz występujące między nimi oddziaływania. Aby prawidłowo ująć to zagadnienie, analiza powinna więc wyodrębnić przede wszystkim te podmioty, które wykorzystując przestrzeń teleinformatyczną, dążą do realizacji określonych interesów, uciekając się przy tym do cyberataków bądź innej aktywności szkodliwej z perspektywy bezpieczeństwa narodowego i międzynarodowego. Klasyfikacja powinna zatem wziąć pod uwagę dwie grupy czynników: po pierwsze stopień organizacji podmiotów, czyli skoordynowania i uporządkowania poszczególnych elementów struktury, aby osiągnąć wyznaczony cel (Czermiński, Grzybowski, Ficoń, 1999: 43—45), po drugie zaś właśnie te cele, a szerzej: motywacje przeprowadzanych cyberataków.

W literaturze przedmiotu istnieje wiele klasyfikacji szkodliwych podmiotów funkcjonujących w cyberprzestrzeni, choć stosunkowo rzadko poświęca się temu zagadnieniu odpowiedni wysiłek w celu dokładnego ich zdefiniowania. Krzysztof Liedel i Paulina Piasecka zwrócili np. w tym kontekście uwagę na znaczenie podmiotowości prawnomiędzynarodowej, przez którą można rozumieć posiadanie zdolności prawnej (zdolności do posiadania praw i obowiązków) oraz zdolności do czynności prawnych (możliwość bezpośredniego zaciągania praw i obowiązków) (Bierzanek, Symonides, 2002: 117). Stwierdzili oni, iż w sieci: „poza podmiotami państwowymi mamy do czynienia z podmiotami niepaństwowymi, takimi jak międzynarodowe korporacje, grupy wpływające na postępowanie rządów czy grupy nielegalne, w tym zorganizowane grupy przestępcze i organizacje terrorystyczne". Słusznie przy tym zauważyli, iż „fakt wejścia do międzynarodowej rozgrywki takich aktorów pociągnął za sobą jej deregulację" (Liedel, Piasecka, 2011: 16). Stosunkowo proste podejście zaprezentował Andrew Cutts (2009), który do podmiotów funkcjonujących w sieci zaliczył hakerów, grupy przestępcze, terrorystów oraz państwa. W bardzo ciekawy i kompleksowy sposób podszedł natomiast do tego zagadnienia Marcin Terlikowski (2009: 96), według którego

> na pierwszym miejscu, ze względu na największy potencjał i możliwości działania, postawić trzeba państwa (ich siły zbrojne i służby), które mogą angażować się w działania z zakresu walki informacyjnej, zarówno w czasie konfliktów, jak i w okresie pokoju. Jednak ataki elektroniczne mogą też być narzędziem osiągania różnorodnych celów także przez podmioty pozapaństwowe. Decyduje o tym przede wszystkim powszechny dostęp do różnych systemów ICT i dynamiczny wzrost liczby osób o pogłębionej wiedzy informatycznej. Sprawcami ataków mogą być zatem nielegalne organizacje, stawia-

> jące sobie cele polityczne (np. grupy rebelianckie, terrorystyczne), grupy przestępcze (motywowane chęcią zysku ekonomicznego), organizacje propagujące określone ideologie, przekonania czy wierzenia (istniejące przeważnie legalnie, lecz uciekające się do niezgodnych z prawem działań, np. ruchy społeczne i polityczne, stowarzyszenia, także sekty religijne), a wreszcie niesformalizowane grupy osób, a nawet jednostki.

W tym kontekście podkreślił autor znaczenie trzech grup: hakerów, haktywistów oraz cyberterrorystów. Można odwołać się również do słów Freda Schreiera (2015: 8—9), który wyróżnił kilka rodzajów szkodliwych podmiotów: zatrudnianych przez rządy państw „legalnych hakerów", „cyberchuliganów" utożsamianych z motywowanymi politycznie haktywistami, cyberprzestępców i komputerowych szpiegów.

W interesujący sposób podeszli do tego zagadnienia Carol Meyers, Sarah Powers i Daniel Faissol (2009: 8). Ich zdaniem należałoby wyróżnić następujące grupy:

- nowicjuszy (*newbies*) i *scripts kiddies*, motywowanych nudą, poszukiwaniem emocji — stanowią niski poziom zagrożenia,
- haktywistów i politycznych aktywistów, motywowanych chęcią promocji określonych postulatów politycznych — średni poziom zagrożenia,
- *cyberpunków*, *crasherów*, chuliganów, motywowanych chęcią uzyskania prestiżu, korzyści osobistych bądź potrzebą silnych emocji — średni poziom zagrożenia,
- użytkowników systemów i sieci, atakujących je od środka z potrzeby zemsty lub uzyskania korzyści osobistych — wysoki poziom zagrożenia,
- programistów poszukujących prestiżu, zemsty lub szacunku w swoim środowisku — średni poziom zagrożenia,
- hakerów starej daty, *sneakerów*, motywowanych określonymi wartościami etycznymi oraz chęcią nauki — bardzo niski poziom zagrożenia,
- profesjonalnych hakerów zwanych czarnymi kapeluszami (*black hat hackers*), dokonujących ataków w imię zemsty lub korzyści osobistych — bardzo wysoki poziom zagrożenia,
- cyberterrorystów, motywowanych określoną ideologią i czasami opłacanych przez państwa — bardzo wysoki poziom zagrożenia[1].

Bardzo ciekawą i spójną typologię przedstawili Piotr Sienkiewicz oraz Halina Świeboda, analizując to zagadnienie wzięli bowiem pod uwagę dwa wspomniane wyżej czynniki: stopień organizacji podmiotu oraz jego motywacje. Uwidoczniło się to w zaproponowanym przez nich podziale zagrożeń bezpieczeństwa teleinformatycznego na ustrukturalizowane i nieustrukturalizowane[2]. W pierw-

[1] Zob. także: Rattray, Healey, 2011.

[2] Przez ustrukturalizowanie można rozumieć posiadanie wewnętrznej struktury, w tym zbioru reguł organizacyjnych, podziału pracy, funkcji, ról. Zob. Kurowski, 2006: 36.

szej grupie wyróżnili oni państwa, w tym ich wyspecjalizowane struktury, terrorystów oraz jednostki transnarodowe, takie jak np. międzynarodowe grupy przestępcze. W skład drugiej grupy wchodzi zdaniem autorów szeroka gama podmiotów, w tym: przestępcy, hakerzy, krakerzy[3], wandale oraz frustraci. Piotr Sienkiewicz i Halina Świeboda (2006: 10) proponując tego typu podział, wskazywali więc pośrednio, że odmienne konsekwencje będzie miał atak przeprowadzony przez pojedynczego przestępcę, a inny włamanie przygotowane i przeprowadzone przez służby obcego państwa.

Wskazana wyżej klasyfikacja szkodliwych podmiotów funkcjonujących w przestrzeni teleinformatycznej zdaje się bardzo przydatna jako podstawa dalszych rozważań poświęconych cyberzagrożeniom dla bezpieczeństwa państw. Niemniej można byłoby dokonać pewnej ograniczonej modyfikacji tej typologii, tak aby pełniej oddawała prawnomiędzynarodowy wymiar tych wyzwań. Przede wszystkim wydaje się, iż obserwując wydarzenia ostatnich lat, a w szczególności coraz większe zainteresowanie NATO i UE cyberbezpieczeństwem, należałoby poszerzyć tę klasyfikację właśnie o organizacje międzynarodowe, przez które rozumie się „zrzeszenia państw powołane do życia dla realizowania zadań określonych w statucie" (Bierzanek, Symonides, 2002: 285). Mimo zasadniczej trudności współpracy międzynarodowej na początku XXI wieku nastąpił wyraźny postęp w tym zakresie[4]. Drugą kategorią zagrożeń ustrukturalizowanych zgodnie z propozycją Piotra Sienkiewicza i Haliny Świebody powinny być wysoce zorganizowane podmioty pozapaństwowe, takie jak organizacje terrorystyczne[5], przestępcze[6] bądź inne nielegalne grupy posiadające strukturę hierarchiczną oraz zróżnicowane cele, np. polityczne, religijne, gospodarcze lub ideologiczne. Być może w przyszłości do tej grupy należałoby zaliczyć także transnarodowe korporacje: współcześnie wiele z nich, szczególnie z sektora IT, posiada potencjał porównywalny lub przewyższający część państw, zarówno z punktu widzenia zasobów ludzkich, posiadanych technologii, jak i *know-how*. Jest on co prawda wykorzystywany głównie do ochrony systemów teleinformatycznych i zawartych w nich danych przed aktami sabotażu, nie można jednak wykluczyć, odwo-

[3] Szerzej na ten temat w rozdziale poświęconym hakingowi.

[4] Przykładem może być kooperacja amerykańsko-izraelska w tej dziedzinie. Zob. *United States-Israel*, 2012.

[5] Można ją zdefiniować jako organizację, której działalność ma charakter terrorystyczny. W literaturze przedmiotu funkcjonuje wiele definicji tego pojęcia. Jedną z najciekawszych jest definicja Departamentu Sprawiedliwości USA, która zakłada, iż jest to: „gwałtowne kryminalne zachowanie, najwyraźniej mające na celu: 1 — zastraszyć i zmuszać ludność cywilną; 2 — wpłynąć na sposób sprawowania władzy przez zastraszenie i przymus; lub 3 — wpłynąć na sposób sprawowania rządów przez zamach lub porwanie". Za: Wojciechowski, 2009: 57.

[6] Do cech organizacji przestępczej Wojciech Kurowski (2006: 36—37) zaliczył m.in. celowe zorientowanie, ustrukturalizowanie, posiadanie systemu sterującego, rozmyślne zachowanie, ekwifinalność, współdziałanie z otoczeniem, zdolność do samoorganizacji, nastawienie na działania przestępcze, wewnętrzną dyscyplinę i kontrolę czy użycie przemocy.

łując się chociażby do bogatej historii szpiegostwa przemysłowego, iż korporacje będą podejmowały (lub już podejmują) działania ofensywne związane np. z nielegalnym zbieraniem wrażliwych informacji[7].

Do stanowiących wysokie zagrożenie podmiotów w cyberprzestrzeni można zatem zaliczyć:

- państwa i ich organizacje,
- wysoce zorganizowane, nielegalne podmioty pozapaństwowe, w tym m.in.:
  — organizacje terrorystyczne,
  — organizacje przestępcze,
  — grupy rebelianckie,
- wysoce zorganizowane, legalne podmioty pozapaństwowe, takie jak korporacje transnarodowe, szczególnie z sektora IT.

Wydaje się, iż nieco inaczej można by również podejść do nieustrukturalizowanych podmiotów będących źródłem zagrożeń w cyberprzestrzeni. Z pewnością należy się zgodzić, iż do tej grupy należy zaliczyć szeroką gamę przestępców działających w sieci. Trzeba przy tym pamiętać, iż istnieje zasadnicza różnica między pojedynczymi kryminalistami bądź ich małymi grupami a organizacjami przestępczymi, których skala działań jest zupełnie inna, przez co można je zaliczyć do wyzwań ustrukturalizowanych. W tym kontekście warto podkreślić, iż przestępcy komputerowi należą do kategorii wyjątkowo szerokiej (zob. Siwicki, 2013), dlatego przyjęto węższe rozumienie tego terminu, które obejmuje tylko takie szkodliwe działania w sieci, których celem jest uzyskanie korzyści materialnych z tego procederu. Oprócz przestępców do podmiotów nisko zorganizowanych należy z pewnością zaliczyć hakerów (w tym krakerów), będących historycznie najstarszą grupą łamiącą zabezpieczenia komputerowe. Od przestępców *sensu stricto* odróżniają ich odmienne i często bardzo zróżnicowane motywacje, wynikające m.in. z chęci rozwoju indywidualnych umiejętności czy uzyskania i/lub opublikowania określonych informacji (Fötinger, Ziegler, [b.r.w.], s. 8). Na przełomie lat 80. i 90. ze środowiska hakerów, kładącego wówczas silny nacisk na aspekty etyczne, wyodrębniła się grupa określana mianem haktywistów. Różniła się ona od protoplastów przede wszystkim jeszcze większym naciskiem na aspekty ideologiczne. Pierwsi haktywiści byli *de facto* hakerami, którzy zaczęli wykorzystywać swoje umiejętności programistyczne w celu promowania określonych poglądów, postaw czy wartości, głównie o charakterze politycznym (Hampson, 2012: 514—517). Na przełomie XX i XXI wieku wśród nich wykształciła się grupa określana przez François Pageta mianem „cyberwojowników". Od haktywistów różnią się oni przede wszystkim nieco innymi motywacjami. W przypadku tych pierwszych mają one z reguły charakter uni-

[7] Zob. Fitchett, 1995; V. Allen: *Google finally admits that its Street View cars DID take emails and passwords from computers*. MailOnline, 28.10.2010: www.dailymail.co.uk/sciencetech/article-1323310/Google-admits-Street-View-cars-DID-emails-passwords-computers.html; dostęp: 22.08.2014.

wersalny, w przypadku drugich wynikają z pobudek, które można określić mianem narodowych, patriotycznych. Haktywiści starają się więc promować np. takie wartości, jak prawa człowieka, działania „cyberwojowników" mają natomiast głównie kontekst międzypaństwowy, który może się przejawiać atakami na strony internetowe państwa, które znajduje się w sporze politycznym z krajem ich pochodzenia (Paget, 2012: 4). Należy również wskazać na szeroką grupę pozostałych, nieustrukturalizowanych podmiotów, do której można zaliczyć posiadających różnorodną motywację amatorów. Będą to więc np. *script kiddies*, którzy nie posiadając własnych umiejętności, wykorzystują do cyberataków programy i skrypty opracowane przez innych, bardziej utalentowanych programistów. Za Piotrem Sienkiewiczem i Haliną Świebodą do tej kategorii należałoby również zaliczyć wszelkiej maści wandali i frustratów, podejmujących niezorganizowane i stosunkowo niegroźne próby szkodzenia innym użytkownikom Internetu. Tym samym do stanowiących zagrożenie podmiotów nieustrukturalizowanych można zaliczyć motywowanych korzyściami osobistymi przestępców, hakerów, haktywistów, „cyberwojowników" oraz amatorów, w tym np. *scripts kiddies*.

Na tym tle widać więc wyraźnie, iż cyberprzestrzeń stała się domeną szkodliwej działalności, której źródeł należy upatrywać na wielu płaszczyznach, począwszy od jednostek, kończąc na wysoce zorganizowanych strukturach państwowych i pozapaństwowych. Warto jednak pamiętać, iż granica między nimi bywa często bardzo płynna, a ponadto wyodrębnienie najważniejszych podmiotów działających w cyberprzestrzeni nie oznacza automatycznie zrozumienia wynikających z ich aktywności zagrożeń.

3.2. Metody cyberataków

Podejmując próbę omówienia najpoważniejszych form wyzwań dla bezpieczeństwa teleinformatycznego, należałoby również odnieść się do właściwości technicznych samych cyberataków. Na wstępie warto wyjaśnić, jak należy rozumieć ten termin. Jego intuicyjna interpretacja wydaje się dość oczywista, jednak w świetle omawianych zagadnień powinno się go jednoznacznie zdefiniować. W literaturze specjalistycznej funkcjonuje równolegle wiele propozycji w tym zakresie. Zdaniem autorów *Tallinn Manual on the International Law Applicable to Cyber Warfare* jest to „cyberoperacja, zarówno ofensywna, jak i defensywna, która powinna przynieść rany lub śmierć osobom lub uszkodzenia bądź zniszczenia obiektom" (Schmitt, ed., 2013: 92). Klaus-Peter Saalbach (2013: 4—5) uznał je za „ataki na komputery, informacje, sieci i systemy zależne od komputerów". Wiele definicji tego pojęcia wypracowała amerykańska armia. Według

pierwszej z nich jest to „wrogi akt przy wykorzystaniu komputera lub związanych z nim sieci lub systemów, zmierzający do zakłócenia i/lub zniszczenia krytycznych cybersystemów przeciwnika, zasobów lub funkcji". W innym ujęciu przygotowanym przez US Army cyberatak scharakteryzowano jako „działania podjęte za pomocą sieci komputerowych w celu zablokowania, osłabienia, zakłócenia lub zniszczenia informacji znajdujących się na komputerach i w sieciach komputerowych" (Cartwright, 2010: 3—6). Często wykorzystuje się także szersze podejście, które stwierdza, iż jest to „wykorzystanie operacji w sieciach komputerowych (Computer Network Operations) z zamiarem zablokowania przeciwnikowi możliwości efektywnego wykorzystania jego komputerów, systemów informacyjnych oraz sieci, zabezpieczając jednocześnie skuteczne działanie własnych komputerów, systemów informacyjnych oraz sieci" (za: Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel, 2012: 826). Można również wspomnieć o dorobku amerykańskiej National Research Council, która określiła je jako „celowe działanie zmierzające do zmiany, zniszczenia, zwiedzenia, osłabienia lub zniszczenia systemów komputerowych, sieci bądź informacji i/lub programów obecnych bądź przepływających przez te systemy i sieci" (Ibidem, s. 825). Warto również przytoczyć interpretację Szanghajskiej Organizacji Współpracy, która zaliczyła do cyberataków także wszelkie działania psychologiczne online (Ibidem, s. 822—826).

Wszystkie powyższe definicje mają jednak pewne wady. Interpretacja Klausa-Petera Saalbacha wydaje się zbyt ogólna i mało konkretna. Z kolei pozostałe, w tym te przygotowane przez autorów *Tallinn Manual on the International Law Applicable to Cyber Warfare* oraz armię amerykańską, pomijają wszelkie przedsięwzięcia, których celem jest nie zniszczenie bądź zakłócenie informacji, lecz jej kradzież[8]. Trzeba przy tym pamiętać, iż specjaliści natowskiego Centrum Doskonalenia Cyberobrony (CCD COE) traktują cyberszpiegostwo jako osobną kategorię, nie zawierającą się w pojęciu cyberataku (Schmitt, ed., 2013: 158).

Na tej podstawie cyberatak można by więc zdefiniować jako wrogie wykorzystanie komputerów, ich sieci oraz innych, pokrewnych technologii i urządzeń (tele)informatycznych, którego celem jest zablokowanie, zakłócenie, zniszczenie lub uzyskanie informacji znajdujących się w sieciach i systemach teleinformatycznych bądź w innych urządzeniach wykorzystujących ICT; zablokowanie, zakłócenie, przejęcie kontroli lub zniszczenie samych sieci i systemów teleinformatycznych bądź innych urządzeń wykorzystujących te technologie. Takie rozumienie tego terminu pozwala dostrzec, iż celem cyberataków nie musi być dokonanie określonych zniszczeń lub zakłóceń w wymiarze materialnym czy niematerialnym, ale także zdobycie określonych informacji w formie cyfrowej, na co często nie zwraca się uwagi.

[8] Szerzej na ten temat: Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel, 2012: 817—886.

Mając na uwadze powyższe rozważania, warto zauważyć, iż istnieje różnica między technikami a środkami cyberataków. Przez techniki należałoby rozumieć sposoby uzyskiwania dostępu do zabezpieczonych danych komputerowych, środki natomiast są swoistymi narzędziami w nich wykorzystywanymi. Razem składają się na metody cyberataków. Analizując to zagadnienie, warto podkreślić, iż w ciągu kilku dekad, które upłynęły od pierwszych bardziej zorganizowanych prób włamań komputerowych, doszło do niebywałego postępu w tej dziedzinie. Obecnie rozwój metod cyberataków jest niezwykle dynamiczny, co wiąże się głównie z trzema kwestiami. Przede wszystkim, o czym wspomniano już wcześniej, współcześnie następuje szybki postęp zarówno w rozwoju technologii komputerowych (*hardware'u*), jak i wykorzystywanego oprogramowania. Ze względu na narastającą rywalizację ich producentów wypuszczane na rynek produkty niestety nie zawsze są w pełni przetestowane, przez co umożliwiają przestępcom wykorzystanie ich luk (*exploit*). Drugi powód wiąże się z rosnącym poziomem skomplikowania rozwiązań technologicznych w tej dziedzinie, przez co zapewnienie skutecznych zabezpieczeń jest coraz trudniejsze. Trzeci powód wydaje się natomiast bardziej prozaiczny. Abstrahując od niedoskonałości systemów komputerowych, należy podkreślić, iż to samo tyczy się obsługujących ich użytkowników, jeszcze w XX wieku przestępcy komputerowi dostrzegli, iż najsłabszym ogniwem zabezpieczeń jest bowiem właśnie człowiek.

Na tym tle należy podkreślić, iż istnieje wiele naukowych klasyfikacji cyberataków. Do najprostszych należy podział na ataki o charakterze pasywnym oraz aktywnym[9]. Inna popularna klasyfikacja wyróżnia tzw. ataki dnia zero i ataki dnia następnego. Najbardziej skuteczne są te pierwsze, które wykorzystują nie odkryty jeszcze błąd w systemie lub określonej aplikacji. Składają się one z dwóch etapów: najpierw następuje odnalezienie danej słabości, po czym dokonuje się innowacyjnego, wcześniej niespotykanego włamania. Ataki dnia następnego wykorzystują natomiast odkryte już luki w zabezpieczeniach w nadziei, iż administratorzy nie zdążyli ich jeszcze naprawić (Jordan, 2011: 35—41).

Nieco bardziej skomplikowaną typologię zaproponowali Simon Hansman i Ray Hunt (2005: 31—43), według których można cyberataki podzielić ze względu na: wektor ataku (czyli metody, za pomocą której szkodliwy kod trafia do źródła), cel (sprzęt bądź oprogramowanie), luki bezpieczeństwa oraz wyniki ataku.

Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta oraz Qishi Wu (2009) swoją klasyfikację oparli na następujących kategoriach: wektor, czyli stosowane metody, rezultat operacyjny, obrona, rezultat informacyjny oraz cel ataku.

[9] M. Matthews: *Network Security Attack: Active/Passive Comparison*. Bright Hub, 27.01.2011: www.brighthub.com/computing/smb-security/articles/104551.aspx; dostęp: 13.08.2014.

Maria Kjaerland wyodrębniła z kolei ataki na podstawie czterech kryteriów: źródeł, metod operacyjnych (wykorzystanych technik i środków), skutków oraz obiektu ataku (Kjaerland, 2006: 522—538; 2005: 105—120)[10].

Z perspektywy prowadzonej analizy najbardziej przydatny wydaje się podział ze względu na stosowane metody operacyjne, czyli środki i techniki cyberataków. Badając je z tej perspektywy, należałoby rozpocząć od zastosowania złośliwego oprogramowania, które można podzielić na kilka typów. Pierwszym są wirusy komputerowe. Po raz pierwszy termin ten został wykorzystany w 1983 roku przez Fredericka Cohena i Lena Adelmana. Wirus utożsamia się często z programem, który może się autonomicznie kopiować i zarażać pliki systemowe bez wiedzy użytkownika. Może się on rozprzestrzeniać na wiele sposobów, w tym np. poprzez dowolną sieć komputerową, Internet bądź nośniki danych (m.in. pamięci USB)[11]. Ciekawą definicję tego pojęcia sformułował John McAfee, który stwierdził, iż jest to „program komputerowy stworzony, aby zarażać inne programy swoimi kopiami. Posiada możliwość klonowania się […], stale poszukując nowych środowisk żywicieli" (McAfee, Haynes, 1989: 1; Bógdał-Brzezińska, Gawrycki, 2003: 146). Pierwszym programem tego typu był prawdopodobnie *Creeper*, napisany jeszcze w 1971 roku przez Boba Thomasa z BBN Technologies. W ciągu kolejnej dekady powstało ich jeszcze kilka, były one jednak stosunkowo niegroźne. Poważniejsze próby na tym tle zaczęły być podejmowane dopiero w latach 80. W 1982 roku powstał *Elk Cloner*, który rozprzestrzeniał się na komputerach typu Apple II za pomocą dyskietek. Był nieszkodliwy, wyświetlając jedynie na monitorze tekst: *It will get on all your disks. It will infiltrate your chips. Yes, it's Cloner!* Niedługo później, w 1983 roku, opracowano eksperymentalnego wirusa napisanego na maszynę z systemem operacyjnym Unix. W kolejnych latach niegroźnych jeszcze programów zaczęło się pojawiać więcej. W 1986 roku Ralf Burger napisał *Virdem*, który swoimi kopiami zarażał pliki systemowe. Rok później pojawiły się m.in. IBM *Christmas Worm*, który replikował się ok. pół miliona razy na godzinę, *Leigh*, który atakował pliki z rozszerzeniem .com, czy nowozelandzki *Stoned*, wyświetlający wiadomość *Your PC is now stoned* [*stoned* 'pod wpływem narkotyków' — M.L.]. Pod koniec lat 80. XX wieku powstał wspomniany *Internet Worm* — jeden z pierwszych wirusów, który poczynił poważne szkody, szczególnie w wymiarze online. Do dynamicznego rozwoju złośliwego oprogramowania doszło jednak dopiero na początku lat 90. XX wieku. Pojawiły się wówczas pierwsze wyspecjalizowane programy, które pozwalały na tworzenie własnych, spersonalizowa-

[10] Za: Meyers, Powers, Faissol, 2009, s. 12—13.

[11] Warto jednak zauważyć, iż według informacji przytoczonych przez Agnieszkę Bógdał-Brzezińską i Marcina Floriana Gawryckiego termin *wirus* w kontekście samoreplikującego się kodu został wykorzystany zdecydowanie wcześniej, bo już w 1970 roku, przez Gregory'ego Benforda. Zob. Meyers, Powers, Faissol, 2009: 14; Bógdał-Brzezińska, Gawrycki, 2003: 145—146; Nikolov, 2000.

nych wirusów. Wówczas oprócz słynnego *Michalangelo* powstały m.in. *Internet Liberation Front*, który zainfekował komputery należące do NASA czy IGM, *Staog* atakujący komputery z systemem operacyjnym Linux oraz polimorficzny *Marburg*. Na przełomie XX i XXI wieku zaczęły się pojawiać pierwsze programy, których celem były pliki HTML oraz PHP[12]. Później wirusy komputerowe zaczęły się coraz bardziej specjalizować, programiści zaczęli je bowiem pisać w taki sposób, aby infekowały jedynie wybrane programy, maszyny bądź usługi. Na tym tle Karsten Johansson wskazał na kilka cech wirusów komputerowych. Jego zdaniem wirusy mogą podlegać mutacji, wymagają zarażonych plików do rozprzestrzeniania się, atakują tylko wybrane ich typy, modyfikują dane ofiary, ich instrukcje są wykonywane, zanim kontrolę uzyska użytkownik, nie infekują dwukrotnie tego samego pliku, symptomy infekcji mogą być niewidoczne bądź odsunięte w czasie[13].

Reasumując ten wątek, warto więc podkreślić, iż użycie wirusów komputerowych jest jedną z najstarszych, najpowszechniejszych oraz najbardziej groźnych metod cyberataków. Mimo coraz większego zaawansowania programów antywirusowych wirusy od lat doprowadzają do ogromnych strat finansowych związanych z awarią systemów teleinformatycznych.

Drugim rodzajem *malware* wykorzystywanych w cyberatakach są robaki (*worms*). Są one samoreplikującymi się programami, które rozprzestrzeniają się za pomocą sieci do innych nosicieli (Yagil, 2002: 71). W przeciwieństwie do wirusów nie muszą się podłączać do istniejących plików i nie wymagają żadnej działalności użytkownika (np. włączenia określonej aplikacji). Ich celem jest raczej zarażenie całej infrastruktury sieciowej, a nie pojedynczych plików. Rozprzestrzeniają się głównie poprzez wykorzystywanie luk w systemach operacyjnych. Często instalują również tzw. tylne drzwi (*backdoor*), dzięki czemu zachowują możliwość zdalnej kontroli komputera. To dzięki nim powstają i funkcjonują omówione już sieci komputerów *botnet*. Robaki mogą się rozprzestrzeniać z bardzo dużą szybkością, co udowodnił m.in. robak SQL *Slammer*, który w 2003 roku w ciągu 12 godzin był w stanie sparaliżować Internet Korei Południowej (Meyers, Powers, Faissol, 2009: 14). Za najsławniejszego i najbardziej skomplikowanego robaka uznaje się z reguły ujawniony w 2010 roku *Stuxnet*, który wykorzystano, aby zainfekować systemy SCADA irańskich ośrodków wzbogacania uranu[14].

---

[12] *History of Virus*. MicroWorld Technologies Inc.: www.mwti.net/products/pdfs/History%20Of%20Virus.pdf; dostęp: 14.08.2013; *Marburg*. F-Secure: www.f-secure.com/v-descs/marburg.shtml; dostęp: 14.08.2013; Meyers, Powers, Faissol, 2009.

[13] K. Johansson: *COMPUTER VIRUSES: The Technology and Evolution of an Artificial Life Form*. 1994, s. 24—32: www.penetrationtest.com/computer_viruses/ComputerViruses-Evolution-KSAJ.pdf; dostęp: 14.08.2013.

[14] Zob. D. Kushner: *The Real Story of Stuxnet*. IEEE Spectrum, 26.02.2013: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet; dostęp: 14.08.2013.

Trzecią kategorią złośliwych programów, które powszechnie wykorzystuje się do cyberataków, są trojany. Jak sama nazwa wskazuje, służą one do włamywania się do komputerów niejako od wewnątrz, analogicznie do legendarnego konia trojańskiego (Yagil, 2002: 70). Według jednej z definicji są to „instrukcje, celowo ukryte w pożądanej części bloku kodu"[15]. Zgodnie z inną *trojan* to „program, w którym zawarty jest złośliwy lub szkodliwy kod, ukryty […] w danych w taki sposób, aby móc przejąć kontrolę i dokonać wybranej formy uszkodzeń"[16]. W ciekawy sposób zagadnienie to wyjaśnili również Agnieszka Bógdał-Brzezińska i Marcin Florian Gawrycki (2003: 149): „program, który może wykonywać niepożądane działania, nieprzewidziane przez użytkownika programu, np. usuwać pliki, ponownie formatować dysk lub przesłać dane do swego twórcy, oczywiście bez zgody użytkownika". Najprościej rzecz ujmując, trojany maskują szkodliwą zawartość wewnątrz pozornie prawidłowego oprogramowania, którego celem jest przejęcie kontroli nad wybranymi funkcjami komputera bądź dokonanie określonych uszkodzeń. Otwierają określone „tylne drzwi" (*backdoors*), które umożliwiają zdalny i nieuprawniony dostęp do danych. W przeciwieństwie do wirusów i robaków trojany nie dokonują samoreplikacji, polegając w pełni na programie nosicielu. Pierwsze konie trojańskie powstały już w połowie lat 70. XX wieku, popularność uzyskały jednak dopiero w latach 90., kiedy wyodrębniło się wiele ich odmian. Interesujący ich przykład stanowią trojany typu *ZeuS* czy *SpyEye*, zaprojektowane w celu włamywania się do kont w systemach e-bankowości. Pierwszy z nich tylko w jednej z akcji posłużył do kradzieży ok. 12 mln dolarów z pięciu największych banków w USA i Wielkiej Brytanii[17].

Wielu ekspertów wyodrębnia również tzw. *rootkity*. Według Davida Harleya oraz Andrew Lee (2009: 4) można je w uproszczeniu zdefiniować jako „zestaw złośliwych narzędzi programowych, które umożliwiają intruzowi ukrycie faktu, że system został przejęty oraz [umożliwiają — M.L.] korzystanie z tego przejęcia". Ich zdaniem celem funkcjonowania *rootkitów* może być utrzymanie uprzywilejowanego dostępu i kontroli nad systemem, umożliwienie osobie i/lub programowi wykorzystania tego dostępu w dowolny sposób oraz ukrycie lub ograniczenie dostępu np. do określonych procesów, plików czy folderów (Ibidem, s. 4). Na przełomie 2009 i 2010 roku *rootkity* odpowiadały za ok. 7% wszystkich infekcji złośliwym oprogramowaniem[18].

[15] *ASM Virus*: http://umcs.maine.edu/~cmeadow/courses/cos335/Asm-Virus.pdf; dostęp: 14.08.2013.

[16] *Viruses, Trojans and Worms...Oh my!* 2006 Technology Leadership Presentation: www.delta.edu/PDFFiles/OIT/Viruses,%20Trojans%20and%20Worms.PDF, dostęp: 14.08.2013.

[17] Zob. Esquibel, Laurenzano, Xiao, Zuvich, 2005; T. Grudziecki: *Cyberataki wczoraj, dziś i jutro*. CERT Polska: www.nask.pl/files/p/Cyberataki_wczoraj_dzis_i_jutro.pdf; dostęp: 14.08.2013; S.M. Bellovin: *Viruses, Trojan Horses, and Worms*. CS-CU, 26.08.2006: www.cs.columbia.edu/~smb/classes/f05/l18.pdf; dostęp: 14.08.2013.

[18] *Some Observations on Rootkits*. Malware Protection Center, 07.01.2010: http://blogs.technet.com/b/mmpc/archive/2010/01/07/some-observations-on-rootkits.aspx; dostęp: 22.08.2014.

Należy zauważyć, iż obecnie rozmaite typologie złośliwego oprogramowania mogą uwzględniać o wiele więcej kategorii, niźli tylko te opisane powyżej. Co więcej, coraz częściej występują programy, które mają zarazem cechy np. robaka i trojana, co komplikuje ich jednoznaczną klasyfikację. Określa się je czasem mianem *blended malware*[19]. W związku z tym obok wspomnianych wyżej typów bardzo często specjaliści wyodrębniają inne rodzaje, w tym m.in.:

1. Programy śledzące (*spyware*) — zainstalowane na komputerze bez wiedzy użytkownika, pozwalają m.in. na zapisywanie całej aktywności sieciowej, co ułatwia m.in. kradzież tożsamości. Korporacja Symantec zaliczyła do nich np. *keyloggery*, dokonujące zapisu wybranych działań dokonywanych przez użytkowników komputera, w tym np. wciśniętych klawiszy[20].
2. *Adware* — wyświetlają na ekranie komputera niechciane reklamy, co z reguły skutkuje znacznym spowolnieniem jego pracy.
3. *Browser hijackers* — bez zgody użytkownika modyfikują ustawienia przeglądarki internetowej[21].
4. *Ransomware* — programy blokujące podstawowe funkcje komputera do momentu wpłacenia przez użytkownika określonej sumy pieniędzy.
5. *Scareware* — stworzone w celu wywołania strachu bądź niepewności; przykładem może być tu program *NightMare* opracowany jeszcze w 1991 roku, który co pięć minut wyświetlał na ekranie komputera wizerunek czaszki[22].

Na tym tle coraz więcej ekspertów wspomina o wykształceniu się swoistych „cyberbroni", na które składają się najbardziej zaawansowane złośliwe programy (zob. Tabansky, 2011, s. 80; Mele, 2013). Pierwszym robakiem tego typu był wspomniany już *Stuxnet*. Na początku drugiej dekady XXI wieku pojawiło się jednak zdecydowanie więcej przykładów tego typu narzędzi. Jednym z nich był program szpiegujący *Duqu*, który został wykryty w 2011 roku. Eksperci Kaspersky Lab udowodnili wówczas, iż jest on spokrewniony ze *Stuxnetem*, został bowiem stworzony w oparciu o platformę *Tilded*. Dzięki uzyskaniu dostępu do serwerów kontroli oraz informacji dotyczących jego architektury pod koniec 2011 roku przestał on istnieć. Później pojawiła się jeszcze jego zmodyfi-

[19] *Enterprise Blended Malware Threats Slip through Traditional Defenses*. Blue Ridge Networks White Paper, 16.03.2012: www.blueridge.com/support/downloads/Enterprise%20Blended%20Malware%20Threat%20WP%20v2.pdf; dostęp: 22.08.2014.

[20] S. Shetty: *Introduction to Spyware Keyloggers*. Symantec, 13.04.2005: www.symantec.com/connect/articles/introduction-spyware-keyloggers; dostęp: 22.08.2014.

[21] Liedel, Piasecka, 2011: 21; Yagil, 2002: 101—102; *Virus Classification*. Tnode: www.tnode.com/VirusClassification; dostęp: 14.08.2013; D. Barroso: *Common Browser Hijacking Techniques*. Terena.org: www.terena.org/activities/tf-csirt/meeting27/barroso-hijacking.pdf; dostęp: 22.08.2014.

[22] T. Grudziecki: *Cyberataki wczoraj, dziś i jutro*, op.cit.; S. Walsh: *Shields Up! How to spot and avoid scareware*. Technology Tell, 12.05.2009: www.technologytell.com/gadgets/47448/shields-up-how-to-spot-and-avoid-scareware; dostęp: 14.08.2013.

kowana wersja, która została wykorzystana do ataku na infrastrukturę krytyczną Iranu. Kolejną „cyberbronią" stał się trojan *Flame*, który pojawił się również w tym kraju w 2012 roku, czyniąc poważne szkody: udało mu się np. skasować dane dotyczące irańskich kontraktów paliwowych, co zablokowało działalność największego składu paliw w tym kraju. Ekspertom IT nie udało się zbadać ani zrozumieć wszystkich zasad działania tego programu, dzięki ich wysiłkom zdołano jednak odkryć niezwykle skomplikowany zestaw narzędzi do przeprowadzania cyberataków, który według Kaspersky Lab powstał w 2008 roku i był wykorzystywany na poziomie państwowym. Był hybrydą łączącą cechy trojana, *backdoora* oraz robaka. Wykonując instrukcje osoby kontrolującej, mógł on m.in. monitorować ruch sieciowy zainfekowanego komputera, rejestrować komunikację głosową za pomocą podłączonych mikrofonów czy pełnić funkcję *keyloggera*. Miał strukturę modułową, dzięki czemu możliwe było poszerzanie jego szkodliwych funkcji. Mógł się też rozprzestrzeniać nie tylko przez Internet, ale także przez sieć LAN i nośniki pamięci. Ciekawostką może być fakt, że podobnie jak *Duqu* był on powiązany z proliferacją robaka *Stuxnet* w 2009 roku. Należy ponadto wspomnieć o dwóch innych cyberbroniach: *Gauss* i *miniFlame*. Pierwsza z nich jest programem cyberszpiegowskim, który potrafi m.in. przechwytywać hasła w przeglądarkach internetowych, wykradać dane z pamięci USB lub z mediów społecznościowych. Podobnie jak wcześniej omówione, został on opracowany przez twórców *Stuxnet* i *Duqu*, jego działalność skupiła się jednak głównie na komputerach znajdujących się w Libanie. Natomiast *miniFlame* jest modułem szpiegującym działającym w ramach *Flame*. Został odkryty w czerwcu 2012 roku. W przeciwieństwie do poprzednich jest dostosowany przede wszystkim do przeprowadzania bardzo precyzyjnych cyberataków ukierunkowanych na uzyskanie określonych danych. Na tym tle zdaniem Aleksandra Gostiewa z Kaspersky Lab można wymienić trzy grupy „cyberbroni": „destruktory", których zadaniem jest niszczenie baz danych (*Wiper*), programy szpiegujące (*Flame*, *Gauss*) oraz najbardziej zaawansowane w tej kategorii narzędzia do cybersabotażu, które mogą dokonać fizycznych szkód (*Stuxnet*)[23].

W tym kontekście, jak zauważył Maciej Ziarek z Kaspersky Lab Polska, od zwykłego złośliwego oprogramowania różnią się one przede wszystkim złożonością kodu oraz zdecydowanie większymi możliwościami wykradania danych. Mając wyższą skuteczność, są wymierzone przede wszystkim w instytucje i agencje państwowe, a nie w pojedynczych użytkowników sieci (Ziarek, 2013: 16—17). Programy te są ponadto na tyle skomplikowane, iż nie mogły zostać stworzone przez pojedynczego programistę: musiały stać za nimi całe zespoły wysokiej klasy specjalistów z zakresu informatyki i matematyki. Na tej podstawie pojawiło się wiele spekulacji wskazujących na fakt, iż za powstaniem całej rodziny „cyberbroni" stał Izrael i/lub Stany Zjednoczone,

[23] Za: Gostiew, 2013, s. 6—8; Zakrzewski, 2013, s. 9—13; Łapiński, 2013, s. 14—15.

które z pewnością miały zarówno motywy ich wykorzystania, jak i odpowiedni potencjał[24].

Charakteryzując szkodliwe oprogramowanie, warto także zauważyć, iż coraz częściej jest ono wykorzystywane do tworzenia wspomnianych już sieci *botnet* (*robot networks*). Generalnie rzecz biorąc, składają się one z zainfekowanych złośliwym oprogramowaniem komputerów, które mogą wykonywać w ukryciu zlecone przez kontrolującego je programistę zadania. Od początku XXI wieku stają się one coraz powszechniejszym i groźniejszym narzędziem w rękach przestępców komputerowych, hakerów, cyberterrorystów czy nawet państw. Mogą być one wykorzystywane do rozsyłania spamu[25], reklam, złośliwego oprogramowania, zdobywania określonych informacji czy też dokonywania cyberataków, np. typu DDoS[26]. Dzięki powszechności Internetu sieci *botnet* potrafią osiągać ogromne rozmiary. Te mniejsze liczą od kilku do kilkudziesięciu tysięcy zainfekowanych komputerów (Xarvester, SpamThru, Wopla, Gheg), mając jednak możliwość wysyłania nawet kilku miliardów e-maili ze spamem dziennie. Standardowe sieci *botnet*, takie jak np. Chameleon, Storm, Bagle czy Kraken, liczą z reguły kilkaset tysięcy komputerów. Te największe i zarazem najgroźniejsze kontrolują nawet miliony komputerów, jak np. słynny Zeus, który w samych tylko Stanach Zjednoczonych kontrolował ok. 3,6 mln komputerów wykorzystywanych m.in. do *phishingu* w mediach społecznościowych (Facebook) czy ataków na użytkowników bankowości elektronicznej[27]. W 2009 roku powstał także BredoLab, który składał się aż z 30 mln komputerów. Na początku 2013 roku odkryto *botnet* Red October. W odróżnieniu od poprzedników jego działalność została wymierzona głównie w polityków, naukowców, wojskowych oraz finansistów, będąc rozwinięciem architektury znanej z sieci Zeus (Zakrzewski A., 2013: 12—13). Jak wcześniej wspomniano, tego typu narzędzia są wykorzystywane zarówno przez pospolitych cyberprzestępców, jak i bardziej zorganizowane

[24] Szerzej zagadnienie to zostanie omówione w kolejnych rozdziałach. Zob. P. Wagenseil: *Are U.S., Israel Behind New Military Malware 'Duqu'?* TechNewsDaily.com, 19.10.2011: www.technewsdaily.com/7252-duqu-origins-stuxnet-questions.html; dostęp: 26.08.2013; D. Jeffers: *The Pandora's Box of Stuxnet, Duqu, and Flame*. PCWorld, 01.06.2012: www.pcworld.com/article/256643/the_pandoras_box_of_stuxnet_duqu_and_flame.html; dostęp: 26.08.2013.

[25] Spam polega na masowym rozsyłaniu wiadomości drogą elektroniczną (e-mail, fora internetowe) bez zgody odbiorców. Jego bardziej szkodliwą odmianą jest *mail bombing* polegający na przekraczaniu pojemności danej skrzynki poczty elektronicznej masową ilością niechcianych wiadomości e-mail. Szerzej: Yagil, 2002: 79.

[26] D. Dagon: *Botnet Detection and Response. The Network is the Infection*. OARC Workshop 2005: www.caida.org/funding/dns-itr/events/200507/slides/oarc0507-Dagon.pdf; dostęp: 26.08.2013.

[27] A. Balapure: *Botnets Unearthed — The ZEUS BOT*. InfoSec, 08.07.2013: http://resources.infosecinstitute.com/botnets-unearthed-the-zeus-bot; dostęp: 26.08.2013; S. Musil: *Zeus botnet steals $47M from European bank customers*. CNET, 05.12.2012: www.cnet.com/news/zeus-botnet-steals-47m-from-european-bank-customers; dostęp: 26.08.2013.

podmioty funkcjonujące w cyberprzestrzeni. Z jednej strony można przytoczyć przykład Jeansona Ancheta, 21-latka, który stworzył liczącą 400 000 komputerów sieć *botnet*. Według niektórych informacji wynajmował on ją przedsiębiorstwom reklamowym działającym w Internecie do rozsyłania spamu i programów typu *adware*, dzięki czemu zarobił ok. 100 000 dolarów. Z drugiej strony narzędzia te są coraz częściej wykorzystywane przez państwa. Największe z tych sieci, liczące kilkadziesiąt milionów jednostek, są zdolne skutecznie zablokować wybrane cele, co może służyć określonym interesom politycznym. Według części ekspertów tego typu sytuacja miała miejsce w trakcie incydentów w Estonii w kwietniu 2007 roku (Bueno, Kashyap, Wosotowsky, 2010)[28].

Kolejną niezwykle popularną i zarazem groźną metodą operacyjną cyberataków jest odmowa dostępu — *denial of service* (DoS). Jej celem jest zablokowanie możliwości skorzystania z określonej usługi lub komputera poprzez zajęcie wszystkich wolnych zasobów. Najczęściej stosowaną techniką jest tu *flooding*, czyli „zalewanie" celu ataku pakietami danych lub zapytaniami ponad limit. Najczęstszymi celami ataków tego typu są m.in. strony internetowe, routery czy konta e-mail. Ataki DoS wyprowadzane z jednego komputera są z reguły mało efektywne, przez co wykształciła się metoda rozproszonej odmowy dostępu (DDoS — Distributed Denial of Service), która polega przede wszystkim na zaatakowaniu ofiary z wielu komputerów jednocześnie, co zdecydowanie wzmacnia skuteczność takiego działania. Wykorzystuje się przy tym omówione wyżej sieci *botnet*. W XXI wieku pojawiły się przypadki, gdy ataki tego typu stały się odpowiednikami wymuszeń haraczy. Przestępcy komputerowi coraz częściej blokują dzięki DDoS określone strony internetowe, oferując ich właścicielom zaprzestanie tego procederu w zamian za uzyskanie określonych korzyści materialnych (Gu, Liu, 2008; Zuckerman, Roberts, McGrady, York, Palfrey, 2010)[29].

Inną ciekawą metodą są ataki sieciowe (*network attacks*), które polegają na manipulowaniu danymi sterującymi transmisją pakietów. Stosuje się tutaj szeroki wachlarz technik. Bardzo rozpowszechnioną jest np. *IP spoofing*, polegający na uzyskaniu nielegalnego dostępu do sieci poprzez podszycie się pod adres IP autoryzowanego komputera. Inne ciekawe to *session hijacking* wykorzystujący pliki *cookie* czy *cross-site scripting* (Meyers, Powers, Faissol, 2009: 16).

Osobno można scharakteryzować bardzo popularne ataki socjotechniczne (oparte na inżynierii społecznej, *social engineering*), które za Krzysztofem Lidermanem (2009: 45) można zdefiniować jako „uzyskanie nieuprawnionego dostępu do informacji poprzez obserwację i oddziaływanie (głównie psycho-

[28] Wilson, 2008, s. 5—6. *Botnets*. Shadowserver Foundation: www.shadowserver.org/wiki/pmwiki.php/Information/Botnets; dostęp: 26.08.2013.

[29] Warto dodać, iż DoS/DDoS wykorzystuje szereg różnorodnych technik, takich jak: *TCP SYN flooding*, *ICMP Smurf flooding* czy *UDP flooding*. Zob. *Denial of Service Attacks*. Columbia University: www.cs.columbia.edu/~smb/classes/f06/l22.pdf; dostęp: 26.08.2013.

logiczne) na użytkownika(ów) systemu teleinformatycznego oraz przeszukiwanie środowiska pracy atakowanego użytkownika". Jedną z jego wersji jest *phishing*. Bywa on rozumiany jako podszywanie się pod określoną osobę lub instytucję w celu wyłudzenia wrażliwych informacji, takich jak np. loginy[30] i hasła do kont bankowych. Od innych cyberataków różni się on przede wszystkim tym, iż *de facto* omija zabezpieczenia komputerowe, bazując przede wszystkim na psychologii i logice relacji międzyludzkich, jest więc szczególnie groźny z punktu widzenia bezpieczeństwa teleinformatycznego. Włamania tego typu mogą więc obejmować spreparowane wiadomości e-mail, które mają skłonić użytkownika do ujawnienia wrażliwych danych lub otworzenia pliku zawierającego złośliwy kod, mogą też polegać na przekierowaniu na zainfekowaną stronę internetową. Bardzo ciekawym przykładem zastosowania tej techniki był wirus *I love you*, który rozprzestrzenił się na całym świecie dzięki znajomości podstawowych mechanizmów relacji międzyludzkich przez jego twórcę[31].

Zgodnie z klasyfikacją Carola Meyersa, Sarah Powers i Daniela Faissola (2009: 16—17) można również wyróżnić ataki na hasła (*password attacks* / *user compromise*). Ich głównym celem jest zdobycie kontroli nad określonym komputerem, usługami bądź danymi dostępnymi z kont użytkowników. Można to osiągać na różne sposoby. Pierwszym z nich jest znajomość danych personalnych określonego użytkownika, czasami hasła i nazwy użytkownika stosowane przez internautów mają bowiem bezpośredni związek z ich życiem prywatnym, posiadane informacje na ten temat mogą zatem pozwolić odgadnąć hasło do konta bądź komputera. Innym sposobem są „ataki słownikowe" (*dictionary attacks*), które — jak wskazuje nazwa — wykorzystują terminy słownikowe jako możliwe hasła. Wreszcie trzeci, bardzo często stosowany, choć prosty sposób, to ataki typu *brute force*: program dokonujący tego typu włamania wprowadza z ogromną szybkością różne losowe sekwencje znaków.

Popularną kategorią jest także *SQL Injection*. Według Krzysztofa Kotowicza jest to „rodzaj ataku na aplikacje internetowe. Polega na tym, że dane od użytkownika pochodzące z URL […], formularzy […], innych elementów […] zostają zmanipulowane tak, że w podatnej aplikacji zostaje wykonane „wstrzyknięte" przez atakującego polecenie SQL"[32]. William G.J. Halfond, Jeremy Viegas i Alessandro Orso wyróżnili następujące podtypy *SQL Injection*: *tautolo-*

[30] Inaczej nazwa użytkownika. Warto dodać, iż przez tzw. logowanie uzyskuje się dostęp do informacji zawartych w systemie informatycznym. Zob. Kępa, 2014: 244.

[31] Zob. Trejderowski, 2013: 11—34; Storch, 2012, s. 8; J. Shi, S. Saleem: *Phishing*: www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic5-final/report.pdf; dostęp: 9.12.2013.

[32] K. Kotowicz: *Kompletny przewodnik po SQL injection dla developerów PHP (i nie tylko)*. The OWASP Foundation, 10.03.2010, s. 6: www.owasp.org; dostęp: 27.08.2014.

gies, *illegal/logically incorrect queries*, *union query*, *piggy-backed queries*, *stored procedures*, *inference* oraz *alternate encodings*[33].

Można ponadto wyróżnić jeszcze dwa specyficzne rodzaje cyberataków. Pierwszym są działania o charakterze materialnym, na które składają się m.in. użycie omówionej już broni elektromagnetycznej (EMP) oraz tzw. *Van Eck phreaking*. Ta druga technika polega na przechwytywaniu sygnałów telekomunikacyjnych oraz danych w formie cyfrowej znajdujących się w pamięci komputera poprzez monitorowanie jego pola elektromagnetycznego. W ten sposób podsłuchujący jest w stanie zdobyć np. wiedzę na temat tego, co aktualnie znajduje się na ekranie komputera, bez konieczności włamywania się do jego systemu. Zagadnieniami tymi zajmuje się m.in. amerykański program TEMPEST (Kuhn, Anderson, 1998: 124—142). Drugą grupą unikalnych metod cyberataków jest zbieranie informacji o zabezpieczeniach komputerowych, które samo w sobie nie wykorzystuje żadnych inwazyjnych technik. Jest to jednak podstawowa działalność, która poprzedza zdecydowaną większość włamań, pozwalając poznać dany system komputerowy oraz zastosowane w nim rozwiązania. Przykładowe techniki w tym zakresie to skanowanie portów sprawdzające, przez które z nich można się włamać, oraz tzw. *packet sniffers*, które monitorują ruch sieciowy (Meyers, Powers, Faissol, 2009: 16—17). Należałoby również pokrótce wspomnieć o błędach w oprogramowaniu lub błędach popełnianych przez samych użytkowników, które mogą zostać wykorzystane do cyberataku. Błędy użytkowników mogą dotyczyć np. nieprawidłowej konfiguracji komputera bądź jego aplikacji, co umożliwia zdalny i nieuprawniony dostęp. Jeśli chodzi zaś o luki w oprogramowaniu, występują ataki stosujące tzw. *kernel flaws* oraz *design flaws*. Pierwsze polegają na wykorzystaniu błędu kodu w systemie operacyjnym komputera, drugie natomiast dotyczą pomyłek, które poczyniono w fazie projektowania danej aplikacji[34].

Powyższe rozważania ze względu na politologiczny charakter pracy stanowią jedynie bardzo uproszczony przegląd popularnych technik i środków cyberataków, co pozwala na pełniejsze zrozumienie najpoważniejszych zagrożeń bezpieczeństwa teleinformatycznego państw z perspektywy ich właściwości technicznych. Należy zaznaczyć, iż zaprezentowane wyżej typy ataków komputerowych stanowią jedynie pewien wycinek wszystkich powszechnie stosowanych metod szkodzenia innym użytkownikom cyberprzestrzeni.

---

[33] W.G.J. Halfond, J. Viegas, A. Orso: *A Classification of SQL Injection Attacks and Countermeasures*. Georgia Institute of Technology 2006: www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf; dostęp: 27.08.2014.

[34] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, Q. Wu: *AVOIDIT: A Cyber Attack Taxonomy*. „Technical Report", CS-09-003. Memphis 2009, s. 3.

3.3. Główne formy zagrożeń dla bezpieczeństwa teleinformatycznego państw[35]

W literaturze specjalistycznej funkcjonuje równolegle wiele typologii zagrożeń teleinformatycznych. Część z nich zwraca uwagę przede wszystkim na podmiot stojący za cyberatakami, co pozwala na zrozumienie ich prawno-politycznych reperkusji. Inne, co omówiono pokrótce w poprzednim podrozdziale, bardzo często koncentrują się na aspektach technicznych, takich jak wykorzystane metody, dokonane zniszczenia czy niezbędne środki ochrony. Wiele prób bierze także pod uwagę przede wszystkim motywacje stojące za szkodliwą działalnością w cyberprzestrzeni (Billo, Chang, 2004). Wszystkie te podejścia przedstawiają jednak cyberzagrożenia w sposób bardzo wycinkowy i ograniczony. Jak więc pisał Andrzej Podraza (2013: 36), „próby jednoznacznego zdefiniowania różnych zagrożeń w cyberprzestrzeni napotykają na szereg problemów. Wynika to przede wszystkim z tego, że do tej pory doświadczenia z atakami w cyberprzestrzeni nie są jednak duże, a nawet w tych sytuacjach podmiotowość sprawców nie jest na ogół znana". Odrębna analiza podmiotów, motywacji bądź właściwości technicznych ma oczywiście fundamentalne znaczenie, nie pozwala jednak na uzyskanie pełniejszego obrazu najważniejszych cech tych zagrożeń. Sytuację dodatkowo komplikuje fakt, iż nie ma zgody środowiska naukowego co do sposobu rozumienia nawet najbardziej oczywistych terminów i pojęć w tej dziedzinie. Świadczy o tym chociażby fakt, iż bardzo swobodnie określa się ten nowy wymiar bezpieczeństwa z punktu widzenia kryterium przedmiotowego. Stosuje się tu, jak wspomniano, nazwy, takie jak *cyberbezpieczeństwo*, *bezpieczeństwo teleinformatyczne*, *bezpieczeństwo komputerowe*, *informatyczne*, *cybernetyczne* lub *informacyjne*[36]. Cały czas trwa również dyskusja dotycząca zasadności stosowania niektórych terminów, takich jak np. *cyberwojna* czy *cyberterroryzm*[37]. Należałoby także zauważyć, iż reprezentanci różnych obszarów wiedzy i dyscyplin naukowych, omawiając te kwestie, wykorzystują częstokroć odrębny aparat pojęciowy, który skupia się jedynie na właściwych im zagadnieniach. Może to prowadzić do ograniczenia perspektywy i rezultatów prowadzonych badań, a co za tym idzie do jednowymiarowej percepcji zagadnień z natury interdyscyplinarnych.

[35] Rozdział ten stanowi rozwinięcie tez zawartych w artykule opublikowanym w numerze 6. czasopisma „E-Politikon". Zob. Lakomy, 2013d.

[36] Zob. np. Libicki, 2007; Hess, ed., 2001; Bendiek, 2012; Carr, 2010; Blane, ed., 2001; Liderman, 2012; Liedel, 2011; Madej, Terlikowski, red., 2009; Lakomy, 2012; Moćkun, 2009.

[37] Clarke, Knake, 2010; Rid, 2012; Bautzmann, 2012; Bufalini, 2012; Shimeall, 2001; *War in the fifth domain*, 2010; Sienkiewicz, 2003; Sienkiewicz, Świeboda, 2009; Liedel, Piasecka, 2011; Lakomy, 2011a; Schweitzer, Siboni, Yogev, 2011.

Chaos terminologiczny na obszarze bezpieczeństwa teleinformatycznego pogłębia równolegle działalność mediów (Wall, 2007: 10—15). Co prawda są one w ostatnich latach w coraz większym stopniu zainteresowane tematyką cyberbezpieczeństwa, odbywa się to jednak kosztem nadmiernego upraszczania omawianych zagadnień i stosowania błędnych lub niedostatecznie wyjaśnionych pojęć. Dziennikarze, poszukując sensacyjnych materiałów, częstokroć charakteryzują te zagadnienia w sposób dalece niewystarczający bądź nieprawdziwy. Dobitnym przykładem tego stanu rzeczy może być nadmierne wykorzystywanie w mediach masowych takich pojęć, jak *cyberterroryzm* lub *cyberwojna*[38]. Po 2007 roku oba stały się niezwykle popularne, czemu z reguły nie towarzyszyła jednak pogłębiona refleksja nad ich rzeczywistym znaczeniem. Sytuację tę trafnie scharakteryzowali Marek Madej i Marcin Terlikowski (2009: 9), według których w ostatnich latach częstokroć

> mówiono o bezpieczeństwie teleinformatycznym (informatycznym), posługując się jednak czasem odmiennymi terminami. Również w stosunku do ich sprawców stosowano, zamiennie i niekonsekwentnie, różnorodne, a ponadto z reguły nieprecyzyjne określenia. Podejmowano także próby klasyfikowania tych zdarzeń, umieszczenia ich na mapie zagrożeń związanych z wykorzystaniem technologii teleinformatycznych. Wysiłki te dawały jednak zazwyczaj obraz nadmiernie uproszczony, uwypuklający jedynie wybrane aspekty poruszanych problemów, a całkowicie pomijający inne.

W tym kontekście dokonanie pełnego przeglądu najważniejszych form zagrożeń dla bezpieczeństwa teleinformatycznego z perspektywy stosunków międzynarodowych, biorącego jednak pod uwagę uwarunkowania techniczne, wydaje się rzeczą niezwykle ważną. Przede wszystkim jest to niezbędne dla samego procesu ich naukowego poznania, a tym samym prawidłowego postrzegania analizowanej rzeczywistości. Jest to zatem kolejny warunek niezbędny do realizacji postawionego we wstępie celu badawczego. Po drugie ma to fundamentalne znaczenie dla wysiłków zmierzających do wypracowania odpowiednich rozwiązań systemowych, obejmujących nie tylko niezbędne środki techniczne, ale także mechanizmy polityczne i prawne, zarówno w wymiarze wewnętrznym, jak i międzynarodowym. Krzysztof Silicki (2009: 203) pisał w tym kontekście, iż podniesienie poziomu bezpieczeństwa teleinformatycznego jest uwarunkowane prawidłowym opisem aktualnej sytuacji na tym obszarze, przez którą rozumiał

[38] Zob. np.: K. Majdan: *Cyberwojna w Rosji. Hakerzy z GhostShell grożą ujawnieniem tajnych dokumentów.* NaTemat.pl: http://natemat.pl/37929,cyberwojna-w-rosji-hakerzy-z-ghostshell-groza-ujawnieniem-tajnych-dokumentow; dostęp: 27.08.2013; R. Kędzierski: *Rosja i USA na skraju cyberwojny? To się już nie zdarzy.* Gazeta.pl, 20.05.2013: http://technologie.gazeta.pl/internet/1,104530,14133760,Rosja_i_USA_na_skraju_cyberwojny__To_sie_juz_nie_zdarzy_.html; dostęp: 27.08.2013.

identyfikację najpoważniejszych przeszkód, ograniczeń i problemów. Po trzecie zaproponowanie podstawowej typologii zagrożeń bezpieczeństwa teleinformatycznego ma fundamentalne znaczenie dla wspomnianej debaty publicznej, która obecnie operuje terminami nieprecyzyjnymi lub zgoła nieprawdziwymi. Ma to ponadto istotne znaczenie z perspektywy prowadzonych od lat prób nawiązania międzynarodowej współpracy w tej dziedzinie. Jednym z głównych powodów, przez które dotychczas nie udało się stworzyć skuteczniejszych mechanizmów kooperacji na obszarze cyberbezpieczeństwa, jest często odmienne postrzeganie zagrożeń teleinformatycznych przez poszczególne państwa[39].

Podejmując próbę budowy nawet najbardziej uproszczonej typologii zagrożeń teleinformatycznych, należałoby więc wyjść od kwestii podstawowej, czyli jej źródeł, które pokrótce omówiono w podrozdziale pierwszym. Podmioty funkcjonujące w cyberprzestrzeni można scharakteryzować w oparciu o trzy kryteria. Pierwszym jest ich status prawno-polityczny, czyli innymi słowy podmiotowość prawa międzynarodowego. Rozstrzygnięcie tej kwestii ma fundamentalne znaczenie dla oceny konsekwencji określonych incydentów nie tylko z perspektywy bezpieczeństwa narodowego, ale także funkcjonowania całego systemu międzynarodowego. Można więc wyróżnić najprościej dwa źródła zagrożeń: posiadające podmiotowość, czyli zdolność prawną i zdolność do czynności prawnych (Bierzanek, Symonides, 2002: 117) — są to głównie państwa i organizacje międzynarodowe oraz nieposiadające podmiotowości, czyli np. organizacje terrorystyczne, zorganizowane grupy przestępcze, inne radykalne grupy, różnorodnie motywowane osoby fizyczne.

Drugim istotnym kryterium może być stopień organizacji. W pracy przyjęto, iż „organizacje tworzą ludzie pełniący określone funkcje i czynności, którzy za pomocą odpowiednio dobranych zasobów i metod działania zdolni są wykonywać wyznaczone zadania" (Czermiński, Grzybowski, Ficoń, 1999: 42—43). Przez stopień organizacji rozumie się występowanie określonego układu hierarchicznego oraz rodzaju struktury, utożsamianych z zestawem relacji zachodzących pomiędzy jej elementami (Ibidem, s. 42—43). Z jednej strony cechy te warunkują posiadany potencjał, z drugiej natomiast wpływają na formułowane cele. Na tym tle można więc wyodrębnić w uproszczeniu podmioty o niskim i wysokim poziomie organizacji. Przez niski poziom organizacji można rozumieć brak hierarchii i struktury organizacyjnej, ich szczątkowe formy i/lub występowanie więzi nieformalnych; mogą to być pojedyncze osoby fizycznie bądź ich niewielkie grupy (hakerzy, haktywiści, cyberprzestępcy). Wysoki poziom organizacji można rozumieć jako występowanie jasno określonej hierarchii oraz rozwiniętej struktury organizacyjnej, która może mieć charakter zarówno formalny,

[39] Za: Lakomy, 2013d: 103—105. Zob. Maurer, 2011; C. Arthur: *Internet remains unregulated after UN treaty blocked*. „The Guardian" 14.12.2012: www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated; dostęp: 27.08.2013.

jak i nieformalny (państwa, ich organizacje, zorganizowane grupy przestępcze, organizacje terrorystyczne).

Trzecie kryterium obejmuje rodzaj posiadanych motywacji, których praktycznym wyrazem są stawiane cele. Ma to zasadnicze znaczenie nie tylko ze względu na sam dobór obiektów ataku (a co za tym idzie stopień zagrożenia dla bezpieczeństwa), ale także sposób reakcji służb państwowych. Zagadnienia te obrazuje tabela 5.

Nie można jednak zapominać o omówionych już wyżej właściwościach technicznych zagrożeń teleinformatycznych. Co prawda z reguły dokonując cyberataków, stosuje się bardzo szeroki wachlarz zaawansowanych środków, jednak dobór celów determinuje również wykorzystywane metody. Częstokroć można dostrzec wyraźne prawidłowości w zastosowaniu określonych technik i narzędzi ataków. Analiza zagrożeń teleinformatycznych bezpieczeństwa państw z perspektywy stosunków międzynarodowych powinna zatem wziąć pod uwagę cztery grupy kryteriów: status prawno-polityczny sprawców, ich stopień organizacji, kierujące nimi motywacje oraz techniczne właściwości incydentów. Tylko tak szerokie podejście pozwoli oddać wielopłaszczyznowy i wielowymiarowy charakter tych problemów.

Tabela 5

Motywacje cyberataków

Rodzaj motywacji	Przykładowe cele
Polityczne	promocja ideologii, postaw lub wartości politycznych; rywalizacja międzypaństwowa i międzynarodowa
Wojskowe	jako podkategoria motywacji politycznych, obejmują wykorzystanie cyberprzestrzeni do realizacji określonych operacji militarnych
Religijne	promocja idei religijnych; nawracanie, walka z „niewiernymi"; zemsta za obrazę religii
Gospodarcze	kradzież technologii; zakłócenie systemu finansowego w celu uzyskania korzyści ekonomicznych
Społeczne	protest związany z występowaniem określonych problemów społecznych
Indywidualne	rozwój umiejętności; poszukiwanie rozrywki; chęć zabicia nudy

Źródło: opracowanie własne.

Bazując na analizie dotychczasowych incydentów teleinformatycznych pod kątem omówionych wyżej czynników, można więc pokusić się o zaproponowanie uproszczonej typologii cyberzagrożeń. Odwołując się do bogatej debaty na ten temat oraz omówionej już klasyfikacji Piotra Sienkiewicza i Haliny Świeboды, należałoby je podzielić na wyzwania ustrukturalizowane i nieustrukturalizowane.

Do zagrożeń ustrukturalizowanych, charakteryzujących się wysokim stopniem organizacji ich źródeł, wysokim stopniem zaawansowania technicznego oraz dominacją motywacji politycznych, wojskowych, religijnych oraz gospodarczych można zaliczyć cyberterroryzm, cyberszpiegostwo i operacje zbrojne w cyberprzestrzeni.

Do zagrożeń nieustrukturalizowanych, posiadających niski stopnień organizacji, stanowiących z reguły mniejsze zagrożenie dla bezpieczeństwa państw, cechujących się dominacją motywacji politycznych, społecznych oraz indywidualnych można zaliczyć haking, haktywizm, „haktywizm patriotyczny" i cyberprzestępczość *sensu stricto* (Lakomy, 2013d: 102—110).

Oczywiście zaproponowana typologia ma w dużej mierze charakter umowny, należy mieć bowiem świadomość, iż interpretacja jakichkolwiek wrogich aktów wymierzonych w bezpieczeństwo państw ma z reguły bardzo płynny i niejednoznaczny charakter. Nawet w tak oczywistych sytuacjach, jak konwencjonalne incydenty zbrojne, decyzja, w jaki sposób je postrzegać na poziomie struktur państwowych, bardzo często ma charakter *stricte* polityczny, uzależniony nie tylko od charakteru tych wydarzeń, ale od szeregu uwarunkowań wewnętrznych i międzynarodowych[40]. Jest to jeszcze bardziej ewidentne w przypadku ataków komputerowych. Ponadto w niezwykle dynamicznym środowisku, jakim jest cyberprzestrzeń, zagrożenia teleinformatyczne podlegają stałej ewolucji. Może dochodzić do wzajemnego przenikania się ich najpoważniejszych form, powstawania nowych bądź modyfikacji starych. Poszczególne zagrożenia mogą również występować wspólnie, tworząc unikalne dla danej sytuacji hybrydy. Nie zmienia to jednak faktu, iż brakuje współcześnie nawet najbardziej podstawowej typologii form zagrożeń teleinformatycznych, która wzięłaby pod uwagę ich wielowymiarowy i wielopłaszczyznowy charakter.

[40] Najdobitniej świadczy o tym fakt, iż nadal nie ma pełnej zgody badaczy co do charakteru i najważniejszych cech współczesnej wojny. Zob. Żurawski vel Grajewski, 2012: 42—79; B. Balcerowicz: *Czym jest współczesna wojna*? Uniwersytet Warszawski: www.pl.ism.uw.edu.pl/index.php?option=com_content&view=article&id=134:prof-dr-hab-bolesaw-balcerowicz-profesor-zwycz&catid=12&Itemid=17; dostęp: 16.09.2013.

3.3.1. Zagrożenia nieustrukturalizowane

3.3.1.1. Haking

Analiza głównych zagrożeń bezpieczeństwa teleinformatycznego państw powinna rozpocząć się od charakterystyki ich historycznych źródeł. Bez wątpienia to właśnie haking jest najstarszą formą wykorzystywania błędów i luk w zabezpieczeniach komputerowych, z której wywodzą się w zasadzie wszystkie pojawiające się współcześnie wyzwania. Jego źródeł należy upatrywać już w latach 60. XX wieku, przed erą ARPANET-u i komputerów domowych, kiedy po raz pierwszy wykorzystano słowo *hack*, prawdopodobnie na Massachussetts Institute of Technology lub Tech Model Railroad Club. Jednym z pierwszych „haków" było odnalezienie przez Williama D. Mathewsa z MIT błędów w oprogramowaniu Multics CTSS na komputerze IBM 7094[41]. Oznaczało ono pierwotnie użycie wysokich umiejętności programistycznych, pozwalających na obejście lub skrócenie określonych operacji wykonywanych przez komputer. Termin *haker* miał więc wówczas pozytywne znaczenie, świadczące o wysokiej specjalizacji informatycznej. Kolejny etap rozwoju tego procederu nastąpił na początku lat 70., kiedy pojawiło się zjawisko *phreakingu*, polegającego na wykorzystaniu luk w zabezpieczeniach sieci telekomunikacyjnych. Za jego prekursora uznaje się Johna Drapera, który dzięki stosowanym przez siebie technikom był w stanie wykonywać darmowe połączenia telefoniczne (zob. Jordan, 2011: 52—54; Levy, 2010: 3—25; Guisnel, 1997a: 118—124).

Do wyodrębnienia hakingu jako zjawiska społecznego doszło jednak zdecydowanie później, dopiero na początku lat 80. XX, co wiązało się z upowszechnieniem komputerów osobistych oraz coraz większym dostępem do sieci. Zarówno domorośli hobbyści, jak i wykształceni programiści pracujący na uniwersytetach coraz częściej zaczęli omijać funkcjonujące wówczas bardzo proste zabezpieczenia komputerowe oraz łączyć się w grupy oparte na wspólnocie zainteresowań. Stopniowo oprócz wymiany doświadczeń grupy te zaczęły się zajmować atakami na instytucje publiczne. Już w 1981 roku w Berlinie powstał Chaos Computer Club, jeden z pierwszych słynnych zespołów hakerskich. W tym samym okresie w USA założono Warelords, które wsławiło się m.in. włamaniami do Białego Domu oraz szeregu największych amerykańskich korporacji. Można także wspomnieć o stworzonej wówczas grupie Legion of Doom. Jej

[41] Yagil, 2002: 64; Siwicki, 2013: 21—22; *Cyber Threats History: The Beginning (1960s).* The Trembling Uterus: http://tremblinguterus.blogspot.com/2012/10/cyber-threats-history-beginning-1960s.html; dostęp: 10.10.2013.

członkowie (m.in. Lex Luthor, The Mentor czy Phiber Optik), dokonując wielu udanych ataków na systemy komputerowe, nie czynili żadnych bezpośrednich szkód. Ich działalność, w tym m.in. publikowanie dzienników technicznych oraz dokumentu *The Conscience of Hacker*, w znacznym stopniu przyczyniła się do rozwoju tego środowiska[42]. Do jednego z pierwszych szeroko komentowanych cyberataków doszło w roku 1982, kiedy grupa 414s włamała się do 60 komputerów należących do instytucji badawczych i państwowych w Stanach Zjednoczonych, w tym m.in. Los Alamos Laboratories oraz Memorial Sloan-Kettering Cancer Center. Seria tego typu incydentów sprawiła, iż sprawą zainteresował się magazyn „Newsweek", zamieszczając na okładce tytuł *Beware: Hackers at play* (Dunn-Cavelty, 2008: 46; Marbach, 1982: 42—48; Hauben, 1989). Problematyka hakerska szybko stała się tak popularna, iż przyciągnęła uwagę producentów filmowych z Hollywood oraz sławnych pisarzy. W 1983 roku ukazał film *War Games* opowiadający o domorosłym programiście, który omal nie wywołał wojny ze Związkiem Radzieckim. Niedługo później na rynku ukazało się kilka pozycji wydawniczych, których głównym tematem był właśnie haking. Jedną z nich była wspomniana już książka Williama Gibsona *Neuromancer*, która przyczyniła się do popularyzacji kultury hakerskiej. Drugą, zdecydowanie ważniejszą pozycją, była natomiast książka Stevena Levy'ego *Hackers: Heroes of the Computer Revolution*[43], która przedstawiła najważniejsze ideologiczne właściwości powstającego ruchu. Hakerzy stopniowo zaczęli siebie postrzegać jako bojowników o wolność informacji oraz racjonalność w debacie publicznej, w związku z tym często mówili o sobie jako o osobach „uzależnionych od informacji" (*information junkie*). Jako subkultura bardzo często utożsamiani byli z wrogami stosującej cenzurę tradycyjnej państwowości, a co za tym idzie środowisko to powszechnie popierało postulaty szeroko pojętej decentralizacji, podkreślało także prawo do „wolności programowania", czego symbolicznym wyrazem stało się powstanie Open Source Movement[44]. To właśnie w tym czasie w świadomości społecznej wykształciło się więc tradycyjne rozumienie słowa *haker* jako osoby, która — jak zauważył Marcin Terlikowski (2009: 98—99) — dzięki „dogłębnej wiedzy informatycznej i indywidualnym zdolnościom potrafiła przełamać zabezpieczenia elektroniczne systemów komputerowych i zdobywać nieuprawniony dostęp do danych w nich przechowywanych".

[42] D. Dickson: *10 Notorious Computer Hackers and Crackers*. Listosaur.com, 16.04.2012: http://listosaur.com/science-a-technology/10-notorious-computer-hackers-and-crackers.html; dostęp: 12.10.2013; *The Legion of Doom/Hackers Technical Journal*. Textfiles.com: http://www.textfiles.com/magazines/LOD; dostęp: 12.10.2013.

[43] Clarke, Clawson, Cordell, 2003; R. Trigaux: *A History of Hacking*. St. Petersburg Times Online, 2000: www.sptimes.com/Hackers/history.hacking.html; dostęp: 28.08.2013.

[44] Zob. *Phrack Pro-Phile on Lex Luthor*. „Phrack" 01.08.1992. T. 40: www.phrack.com/issues.html?issue=40&id=3; dostęp: 12.10.2013; Levy, 2010: 27—38; Jordan, 2011; T. Chance: *The Hacker Ethic and Meaningful Work*. 03.08.2005: http://flosshub.org/system/files/chance.pdf; dostęp: 28.08.2013.

Wraz z postępującą popularyzacją tego procederu środowisko hakerów zaczęło się jednak w tym okresie różnicować. Obok posiadających pewne bariery etyczne hakerów pojawiły się pierwsze jednostki, które zaczęły wykorzystywać swoje wyjątkowe zdolności w celu uzyskania określonych korzyści osobistych, dla rozrywki bądź z nudy. Symbolem tego typu działań stała się historia poszukiwanego w całych Stanach Zjednoczonych Kevina Mitnicka (Yagil, 2002: 82; Gagnon, 2009: 125; Trejderowski, 2013: 36—44). Innym przykładem był Markus Hess, który dokonywał cyberataków na serwery instytucji zachodnich z polecenia radzieckiego KGB. Zaczęły się wówczas pojawiać również zorganizowane grupy wywodzące się ze środowiska hakerów, które miały jednak już odmienne motywacje, głównie o charakterze politycznym, niektórym programistom przestało bowiem wystarczać wykorzystywanie swoich umiejętności jedynie w ramach procesu samodoskonalenia[45]. Warto także wspomnieć, iż w 1988 roku doszło do pierwszego głośnego ataku komputerowego na First National Bank of Chicago, w wyniku czego skradziono ok. 70 mln dolarów[46]. W tym kontekście należy zauważyć, iż mimo oderwania się od głównego nurtu tego środowiska nowych, odrębnych jakościowo grup, pojęcie hakingu nadal było rozumiane bardzo szeroko.

Dojrzałą formę proceder ten osiągnął dopiero kilka lat później. W środowisku specjalistów komputerowych zaczęto stosować wyraźnie sprecyzowane nazewnictwo w odniesieniu do hakerów różniących się stosunkiem do przestrzegania prawa, motywacjami oraz sposobami działania. Wyróżniono tu tzw.:

1. Białe kapelusze (*white hats*), czyli osoby, które kładą silny nacisk na aspekt etyczny swoich działań. Wyznawane przez nich zasady w dużej mierze licują z pierwotną, najbardziej tradycyjną formą hakingu, akcentującą prawo do informacji, wolność programowania i wolność słowa. Przy czym należy zauważyć, iż białe kapelusze starają się zawsze działać w granicach obowiązującego prawa, dokonując cyberataków głównie w celu podniesienia własnych kompetencji, sprawdzenia się. Co więcej, częstokroć ich zamiarem jest poprawa stanu złamanych zabezpieczeń.
2. Szare kapelusze (*grey hats*) dopuszczające łamanie prawa, jednak w tylko w imię wyższych wartości i potrzeb, mogą zatem działać na rzecz podniesienia jakości zabezpieczeń komputerowych, lecz w odróżnieniu od „białych" korzystają z nielegalnych metod i środków. Głównym motywem ich działania pozostaje jednak samodoskonalenie.
3. Czarne kapelusze (*black hats*), utożsamiane często z krakerami. Dokonują oni cyberataków rażąco łamiących obowiązujące prawo i czynią nieuzasad-

[45] Guisnel, 1997a: 132; Lakomy, 2010: 57; T.C. Greene: *Chapter One: Kevin Mitnick's story*. 13.01.2003: www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story; dostęp: 28.08.2013. Za: Lakomy, 2013d: 110—112.

[46] D. Icove, K. Seger, W. VonStorch: *Fighting Computer Crime*. Computer Crime Research Center, 2001—2002: www.crime-research.org/library/crime1.htm; dostęp: 10.10.2013.

nione szkody w systemach i sieciach, do których uzyskali dostęp. Nie działają na rzecz podniesienia stanu zabezpieczeń, a wręcz przeciwnie: częstokroć wiedzę na temat odkrytych luk i błędów przekazują innym hakerom. Od regularnych cyberprzestępców różnią się jednak tym, iż ich aktywność nie ma na celu uzyskania określonych korzyści osobistych, a np. sprawdzenie własnych umiejętności[47].

Odwołując się do wcześniej zaproponowanych kryteriów, należy stwierdzić, iż haking jest zagrożeniem o niskim stopniu organizacji i nie wiąże się zazwyczaj z jakimikolwiek skutkami dla stosunków międzynarodowych, hakerzy bowiem z reguły działają samotnie. Nawet gdy funkcjonują w grupach, mają one charakter nieformalny, oparte są więc głównie na niezhierarchizowanych więziach międzyludzkich, powstałych w wyniku wzajemnego uznania dla reprezentowanych umiejętności programistycznych. Stosują bardzo szeroki i zaawansowany wachlarz metod cyberataków, które jednak rzadko są kierowane przeciwko obiektom mającym istotne znaczenie dla bezpieczeństwa państw. Zazwyczaj samotni hakerzy nie posiadają wystarczającego potencjału, aby poważnie zagrozić np. systemom kontrolującym funkcjonowanie infrastruktury krytycznej czy systemu obronnego. Nawet jeśli takie włamanie zakończyłoby się sukcesem, celem w większości przypadków nie powinno być poważne zaszkodzenie strukturom państwa bądź ludności cywilnej. Za wzorcowy przykład można uznać *casus* hakera Alladyn2, który na początku 2013 roku włamał się do komputerów Kancelarii Prezesa Rady Ministrów RP, Ministerstwa Obrony Narodowej, Kancelarii Prezydenta i Ministerstwa Spraw Zagranicznych. Mimo uzyskanego dostępu nie wykradł on żadnych wrażliwych danych ani nie dokonał poważnych szkód (poza ujawnieniem haseł i nazw użytkownika m.in. do kont e-mail pracowników rządowych). Celem jego działań było — jak twierdził — podniesienie stanu zabezpieczeń polskich instytucji państwowych wobec coraz częstszych ataków ze strony Chin, a także „*fun* i doświadczenie". W wydanym oświadczeniu zadeklarował:

> Pragnę uspokoić CERT oraz inne instytucje rządowe, uprzejmie informuję, że nie było to *'state sponsored attack'*. Więc to nie były chinole i ich APT 1 :) Rok temu się nie udało, tym razem KPRM zdobyty (inne ministerstwa też się załapały na niezamówiony test penetracyjny). Na razie trwa zacieranie śladów, ale za kilka dni pojawi się dowód, że nie był to tylko dostęp do poczty kilku pracowników :)[48].

[47] Harris, Harper, Eagle, Ness, 2008; Gottlieb, 1999. Za: Lakomy, 2013d: 112—113.

[48] *Kancelaria Premiera, MSZ, MON i Kancelaria Prezydenta zhackowane. Wiemy kto stoi za tymi włamaniami*. Niebezpiecznik.pl, 13.03.2013: http://niebezpiecznik.pl/post/kancelaria-premiera-msz-mon-i-kancelaria-prezydenta-zhackowane-wiemy-kto-stoi-za-tymi-wlamaniami; dostęp: 29.08.2013.

Ciekawym przykładem z ostatnich lat była także grupa LulzSec (Lulz Security), będąca grupą hakerów dokonujących głośnych cyberataków głównie „dla zabawy" oraz w celu polepszenia stanu zabezpieczeń komputerowych. Co prawda stali oni również za włamaniami wynikającymi z określonych postulatów politycznych (np. operacja AntiSec), jednak z reguły działalność LulzSec miała charakter *stricte* hakerski. Do najsławniejszych dokonań tej grupy należało złamanie zabezpieczeń serwerów korporacji Sony, Nintendo, CIA oraz amerykańskiego Senatu[49].

Reasumując, haking można uznać za proceder, który polega na wykorzystywaniu rozmaitych zaawansowanych technik i narzędzi cyberataków głównie w celu podniesienia kompetencji, zdobycia doświadczenia. Mogą występować także motywacje poboczne, związane z chęcią poprawy zabezpieczeń komputerowych, promowaniem wolności informacji, wolności słowa, rozrywką bądź dokonaniem nieuzasadnionych zniszczeń. W takim ujęciu haking nie ma szerokiego kontekstu politycznego i nie stanowi szczególnego zagrożenia dla bezpieczeństwa systemów i sieci państwowych. Jest raczej marginalnym wyzwaniem dla bezpieczeństwa narodowego i międzynarodowego, szczególnie biorąc pod uwagę fakt, iż jego skala w porównaniu do głównego nurtu cyberprzestępczości czy haktywizmu jest współcześnie niewielka (zob. Terlikowski, 2009: 98—99).

3.3.1.2. Haktywizm

Haktywizm jako nieustrukturalizowana forma zagrożeń bezpieczeństwa teleinformatycznego wyodrębniła się, jak wspomniano wyżej, z głównego nurtu hakingu już w latach 80. XX wieku. Część hakerów dostrzegła wówczas, iż ich umiejętności mogą być wykorzystane do promowania określonych wartości, postaw i idei, zarówno o charakterze politycznym, jak i społeczno-gospodarczym. Było to niejako naturalne rozwinięcie silnego nacisku na kwestie etyczne pierwotnych form hakingu. To właśnie dlatego wyraźne oddzielenie antypaństwowej ideologii hakerów od działalności pierwszych haktywistów jest zadaniem niezwykle trudnym. Z reguły uznaje się, iż pierwsze cyberataki tego typu przeprowadzono w październiku 1989 roku. Wynikały one z ogólnoświatowego sprzeciwu wobec amerykańskich próbnych wybuchów jądrowych. Komputery NASA oraz Departamentu Energii zostały wówczas zainfekowane robakiem *WANK*, który wyświetlał na ekranie wiadomość: *WORMS AGAINST NUCLEAR KILLERS... Your System Has Been Officially WANKed*. Stworzony prawdopo-

[49] *LulzSec Hacks*. Know Your Meme: http://knowyourmeme.com/memes/events/lulzsec-hacks; dostęp: 29.08.2013.

dobnie w Australii, był to pierwszy w historii robak wykorzystany *stricte* do celów politycznych. Świadomość własnej odrębności haktywiści zaczęli zyskiwać jednak dopiero na początku lat 90. W listopadzie 1994 roku grupa o nazwie Zippies dokonała zorganizowanych ataków DDoS przeciwko brytyjskim instytucjom rządowym w proteście przeciwko zakazowi publicznych festiwali muzyki elektronicznej. Operacja określana mianem *Intervasion of the UK* zablokowała rządowe strony internetowe na ponad tydzień, co świadczyło o jej relatywnym sukcesie. Na tym tle w 1996 roku ukuto termin *haktywizm*, którego po raz pierwszy użył członek utworzonej już w 1984 roku teksańskiej grupy Cult of the Dead Cow. W tym pierwotnym ujęciu za haktywistę uznawano osobę stosującą techniki hakerskie do promocji określonych idei lub postaw politycznych. Warto dodać, iż grupa ta czerpała swoje postulaty głównie z kodu etycznego hakingu. Wychodząc od tak podstawowych kwestii, jak wolność słowa i prawo do informacji, skupiła się na zdecydowanie szerszej kategorii, jaką jest ochrona praw człowieka. Symbolem ich działań stało się wsparcie dla chińskich dysydentów za pomocą cyberataków przeciwko instytucjom państwowym ChRL[50].

Swoją współczesną, bardzo spopularyzowaną formę haktywizm osiągnął dopiero na początku XXI wieku. W 2001 roku opublikowano *Hacktivismo Declaration*, swoisty kodeks postępowania oparty w głównej mierze na *Powszechnej deklaracji praw człowieka*. Zaakcentowano w nim znaczenie wolności słowa i informacji, wskazując zarazem, iż rządy państw w coraz większym stopniu ograniczają je poprzez cenzurę Internetu[51]. Do rozwoju haktywizmu przyczyniło się również powstanie w 2003 roku popularnego serwisu 4chan.org, który stał się kolebką największych organizacji haktywistycznych. To właśnie tutaj powstała grupa Anonymous, która sprawiła, iż haktywizm został dostrzeżony przez opinię publiczną na całym świecie. Po raz pierwszy media zainteresowały się nią szerzej w styczniu 2008 roku, kiedy rozpoczęto Project Chanology, serię ataków komputerowych skierowanych przeciwko Kościołowi Scjentologicznemu. W kolejnych latach aktywność Anonymous przejawiała się włamaniami wymierzonymi m.in. w rządy Ugandy, Turcji, Tunezji, Egiptu czy instytucje zajmujące się prawami autorskimi, w tym np. US Copyright Office[52]. Grupa ta przez pewien czas działała również przeciwko Polsce, co wynikało z podpisania przez rząd Donalda Tuska umowy ACTA[53]. Za apogeum znaczenia haktywizmu uznaje

[50] Zob. T. McCormick: *Hacktivism: A Short History*. „Foreign Policy" 29.04.2013: www.foreignpolicy.com/articles/2013/04/29/hacktivism; dostęp: 29.08.2013; Bógdał-Brzezińska, Gawrycki, 2003: 60—61.

[51] *The Hacktivismo Declaration*. cDc communications, 04.07.2002: www.cultdeadcow.com/cDc_files/declaration.html; dostęp: 29.08.2013.

[52] N. Wolchover: *Best Hacks by the Hacktivist Group 'Anonymous'*. LiveScience, 11.11.2011: www.livescience.com/33599-best-hacks-anonymous-hacktivism.html; dostęp: 29.08.2013.

[53] *Polskie strony rządowe przestały działać. Protest przeciwko ACTA?* Wirtualna Polska, 21.01.2012: http://wiadomosci.wp.pl/kat,1329,title,Polskie-strony-rzadowe-przestaly-dzialac-Protest-przeciwko-ACTA,wid,14187932,wiadomosc.html?ticaid=1100ef&_ticrsn=5; dostęp:

się jednak dopiero arabską wiosnę, w której Internet odegrał fundamentalną rolę, motywowani politycznie programiści dokonywali bowiem masowych ataków na strony internetowe arabskich reżimów autorytarnych, umożliwili także łatwiejszą wymianę informacji między protestującymi w sytuacji rosnącej cenzury sieci (zob. Sterner, 2012). Na tym tle wycinkowym, lecz ciekawym przykładem może być działalność haktywisty określającego się mianem The Jester (th3j35t3r), który w latach 2009—2010 aktywnie zwalczał w Internecie strony islamskich dżihadystów, wykorzystując do tego zestaw narzędzi, które nazwał mianem Xerxes (Zuckerman, Roberts, McGrady i in., 2010: 32).

W tym kontekście od wielu lat środowisko naukowe dyskutuje nad odpowiednim zdefiniowaniem tego zjawiska. Jedną z pierwszych naukowych propozycji wysunęła Dorothy E. Denning, która stwierdziła, iż jest to „konwergencja hakingu i aktywizmu, w której haking odnosi się do wykorzystywania komputerów w sposób nietypowy i często nielegalny, z reguły z wykorzystaniem specjalistycznego oprogramowania". Jej zdaniem „haktywizm obejmuje elektroniczne nieposłuszeństwo obywatelskie, przenosząc metody obywatelskiego nieposłuszeństwa w cyberprzestrzeń"[54]. Robert Vamosi uznał go za „użycie narzędzi cyfrowych" w celach politycznych. Określił go ponadto jako kombinację hakingu oraz społecznego aktywizmu[55]. Tim Jordan oraz Paul Taylor zauważyli, iż jest to „połączenie technik hakerskich ze […] strategiami komunikacyjnymi politycznego aktywizmu, zgodnie z agendą nowego, zglobalizowanego ruchu" (Jordan, Taylor, 2004). Graham Meikle zdefiniował haktywizm jako „małżeństwo politycznego aktywizmu i komputerowego hakerstwa" (Fitri, 2011: 7). Maura Conway zauważyła natomiast, że „haktywiści, jakkolwiek wykorzystują Internet do akcji politycznych, nie są cyberterrorystami. Postrzegają się jako spadkobiercy tych, którzy wykorzystują metody wykroczeń i blokad w świecie realnych protestów. Są w większości zaangażowani w zakłócanie [systemów — M.L.], a nie [ich — M.L.] niszczenie" (Ibidem, s. 7). Warto wspomnieć również o grupie badaczy, która zajęła stanowisko, iż proceder ten może obejmować wirtualne działania każdego aktora niepaństwowego w celu zwrócenia uwagi opinii publicznej na określony problem polityczny lub wyrażenia niezadowolenia (Ibidem, s. 2, 6—8). Z kolei Mark G. Milone (2002: 385—386) uznał, że haktywista, wykorzystując te same narzędzia co haker, działa w celu zwrócenia uwagi na

29.08.2013; M. Casserly: *What is Hacktivism? A short history of Anonymous, Lulzsec and the Arab Spring*. PC Advisor, 03.12.2012: www.pcadvisor.co.uk/features/internet/3414409/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring; dostęp: 29.08.2013; *Wikileaks Infowar was not the first online protest action*. „Media Alternatives": http://medialternatives.blogetery.com/2010/12/15/intervasion-supports-anonymous; dostęp: 29.08.2013.

[54] Za: J.L.C. Thomas: *Ethics of Hacktivism*, Aribo.eu, 12.01.2001: www.aribo.eu/wp-content/uploads/2010/12/Thomas_2001-copy.pdf; dostęp: 13.02.2013.

[55] R. Vamosi: *How Hacktivism Affect Us All*. PCWorld, 06.09.2011: www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html; dostęp: 12.10.2013.

określony cel polityczny lub społeczny. Na gruncie rodzimej literatury specjalistycznej inne rozumienie tego pojęcia zaproponował Marcin Terlikowski (2009: 105), którego zdaniem współcześnie główną motywacją haktywizmu są bieżące problemy polityczne, cyberataki natomiast stały się kolejną formą walki politycznej, „prowadzonej przez członków i sympatyków różnych organizacji". Tomasz Trejderowski (2013: 172) zdefiniował je jako „działania hakerskie mające podłoże lub cele destrukcyjne, ale nie przynoszące żadnych strat lub przynoszące relatywnie minimalne; można do tej grupy zaliczyć blokowanie stron, podmienianie treści, zamieszczanie własnych apeli itp.". Natomiast Agnieszka Bógdał-Brzezińska oraz Marcin Florian Gawrycki (2003: 60) stwierdzili, iż działalność haktywistów „ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócenie uwagi na dany problem".

W tym kontekście można wskazać na kilka zasadniczych cech haktywizmu jako nieustrukturalizowanej formy zagrożeń teleinformatycznych. Przede wszystkim w odróżnieniu od hakingu jest to działalność wyraźnie motywowana polityczne. Haktywiści wykorzystują cyberataki do promocji określonych wartości, postaw lub idei politycznych i społecznych lub aby zwrócić uwagę opinii publicznej na określone problemy. Przy czym świadomość polityczna grup haktywistów w rzeczywistości bywa bardzo niska, a ich aktywność wiąże się z wysuwaniem postulatów mających głównie charakter uniwersalny i globalny. Odwołują się do szeroko pojętych praw człowieka wszystkich generacji, krytycznie postrzegając przejawy ich łamania. Zgodnie z hakerską tradycją za głównego wroga uznają państwa, ich zdaniem coraz bardziej ograniczające swobodę wypowiedzi w Internecie. Powyższe motywacje są konkretyzowane w formułowanych przez nich celach. Dokonują cyberataków wymierzonych głównie w instytucje państwowe, korporacje, partie polityczne, organizacje rządowe i pozarządowe oraz inne zorganizowane podmioty funkcjonujące w sieci. Ze względu na duże znaczenie różnorodnie rozumianych zasad etycznych haktywiści stoją za incydentami, które z natury stanowią niewielkie zagrożenie dla bezpieczeństwa narodowego i międzynarodowego, ich założeniem jest bowiem jak największa widowiskowość akcji, zwrócenie uwagi opinii publicznej, a nie dokonanie trwałych szkód w systemach i usługach, które mogłyby wpłynąć na funkcjonowanie państwa bądź życie obywateli. Takie działanie wymierzone np. w elementy infrastruktury krytycznej miałyby więc skutek odwrotny do zamierzonego. Obiektem ataków są głównie strony internetowe oraz wrażliwe dane, których ujawnienie opinii publicznej mogłoby wpłynąć na charakter debaty publicznej[56]. Haktywiści podejmują także działania, których celem jest ułatwienie swobody wymiany informacji

[56] G. Coleman: *Coleman Discusses „Anonymous" as Civil Disobedience*. Steinhardt School of Culture, Education, and Human Development: http://steinhardt.nyu.edu/news/2011/3/11/Coleman_Discusses_Anonymous_as_Civil_Disobedience, 21.11.2012; dostęp: 1.09.2013.

i opinii w Internecie. Wyrazem tego typu aktywności były np. cyberataki przeprowadzone przez Anonymous na strony polskiego rządu w styczniu 2012 roku czy przeciwko amerykańskim instytucjom po zamknięciu serwisu Megaupload. Po drugie haktywiści działają co prawda raczej w grupach mających określone motywacje i cele, lecz grupy te nie mają ani jasno określonej hierarchii, ani sformalizowanej struktury. Proces podejmowania decyzji odbywa się w nich z reguły na podstawie dyskusji wszystkich członków. Po trzecie należy stwierdzić, iż w wymiarze technicznym haktywiści stosują szeroki wachlarz metod, głównie blokowanie, modyfikacje lub kradzież danych w formie cyfrowej. Częstokroć odwołują się oni do technik DDoS, stanowiących najprostszy sposób paraliżowania usług sieciowych, w tym wybranych portali internetowych. Warto również podkreślić, iż skala haktywizmu w ostatnich latach zdecydowanie wzrosła. Szyld Anonymous, pod którym zaczęli gromadzić się programiści posiadający określone motywacje polityczne, stał się rozpoznawalny na całym świecie. Akcje przeprowadzane przez to środowisko są coraz częściej dostrzegane przez media masowe, wywierają zatem wymierny wpływ na debatę publiczną, a czasami nawet na decyzje elit politycznych (Lakomy, 2013d: 115—117).

Reasumując ten wątek, należy podkreślić, iż haktywizm jest stale ewoluującą i coraz powszechniejszą formą nisko zorganizowanej, szkodliwej działalności w cyberprzestrzeni, nie stanowi on jednak poważniejszego wyzwania dla bezpieczeństwa państw. Co prawda cyberataki przeprowadzane przez tę grupę mogą być czasami uciążliwe dla instytucji publicznych, jednak głównie w wymiarze wizerunkowym.

3.3.1.3. Haktywizm patriotyczny

Analizując nieustrukturalizowane zagrożenia dla bezpieczeństwa teleinformatycznego państw, warto wspomnieć o wyjątkowej formie haktywizmu, na którą uwagę zwrócił m.in. ekspert McAfee Labs, François Paget (2012: 26—27), wyodrębniając w swojej analizie grupę „cyberwojowników", czyli osoby działające w cyberprzestrzeni głównie z pobudek narodowych, wchodzące w skład tzw. cyberarmii, które podejmują się szkodliwej działalności w sieci w imię określonych wartości lub postaw politycznych właściwych danemu państwu lub grupie narodowej. W przeciwieństwie do konwencjonalnych haktywistów, którzy, przynajmniej oficjalnie, reprezentują uniwersalne wartości, „cyberwojownicy" działają w sieci przede wszystkim w imię idei patriotycznych, dzięki czemu ich aktywność częstokroć zyskuje kontekst międzynarodowy, między-

państwowy. Dokonywane przez nich ataki komputerowe towarzyszą zazwyczaj poważnym sporom i kryzysom politycznym lub nawet konfliktom zbrojnym, stanowiąc formę zagrożeń dla bezpieczeństwa teleinformatycznego, która jakościowo różni się od głównego nurtu haktywizmu. Ruch ten można roboczo określić mianem *haktywizmu patriotycznego* ze względu na jego silne związki z wartościami narodowymi, tradycją, rozwojem państwa czy obroną jego interesów na arenie międzynarodowej[57].

Haktywizm patriotyczny jako zjawisko wykształcił się nieco później niż jego tradycyjna forma. Na szerszą skalę pojawił się on dopiero na przełomie XX i XXI wieku. Można tutaj przytoczyć szereg interesujących przykładów, typowych głównie dla krajów azjatyckich. Przede wszystkim należy zauważyć, iż od lat dochodzi do wzajemnych starć między haktywistami Izraela oraz Palestyny, co towarzyszy kolejnym napięciom oraz incydentom zbrojnym w tym regionie. W listopadzie 2012 roku w odpowiedzi na bombardowania Strefy Gazy arabscy „cyberwojownicy" zaatakowali izraelskie strony internetowe aż 44 mln razy[58]. Do podobnych incydentów doszło również we wrześniu 2013 roku, kiedy grupa AnonGhost zaatakowała w ramach operacji *OpIsrael Reborn* wiele stron rządowych tego kraju (Cohen, Hirschauge, 2013). Po drugie od lat dochodzi do bardzo natężonej rywalizacji między haktywistami Indii i Pakistanu w kontekście sporu obu państw o Kaszmir. Grupy patriotycznie motywowanych programistów zgromadzonych m.in. w Pakistan Cyber Army, Pakistan Cyber Pirates czy The United Indian Hackers dokonują masowych cyberataków przeciwko stronom internetowym przeciwnika. Tylko w grudniu 2012 roku dwóch Pakistańczyków włamało się na ok. 300 indyjskich stron WWW[59]. Warto w tym kontekście wspomnieć również o niedawno utworzonej grupie Anonymous Kashmir, która stoi za atakami na indyjskie strony internetowe. We wrześniu i październiku 2013 roku włamała się m.in. na witryny Honda India czy BHSE Delhi. Aktywność ta miała być odpowiedzią na brutalność indyjskiej armii w Kaszmirze. O skali tych „walk" świadczył fakt, iż według źródeł pakistańskich w tym czasie łupem „cyberwojowników" padło ok. 20 000 indyjskich stron internetowych[60]. Intere-

[57] Na znaczenie patriotyzmu jako czynnika mobilizującego internautów do organizowania cyberataków przeciwko innym państwom zwrócili uwagę m.in. Vincent Joubert oraz Gergana Petkova, 2014.

[58] Szerzej w: Geers, 2011: 83; *Mass cyber-war on Israel over Gaza raids*. Al Jazeera, 19.12.2012: www.aljazeera.com/news/middleeast/2012/11/201211197311174613 7.html; dostęp: 2.09.2013.

[59] J. Lee: *300 Indian sites defaced by Pakistani hackers*. Cyber War News, 09.12.2012: www.cyberwarnews.info/2012/12/09/300-indian-sites-defaced-by-pakistani-hackers; dostęp: 2.09.2013; B. Khanna: *India-Pak on Cyber War prior August 15*. „Hindustan Times" 21.08.2012: www.hindustantimes.com/Punjab/Chandigarh/India-Pak-on-Cyber-War-prior-August-15/SP-Article1-917212.aspx; dostęp: 2.09.2013.

[60] *Pakistan Cyber Army*. Facebook: www.facebook.com/PakistanCyberArmyPCA; dostęp: 12.10.2013.

sujący przykład stanowi Iranian Cyber Army, która w kontekście impasu politycznego wokół irańskiego programu atomowego od 2009 roku bierze na cel głównie zachodnie serwisy internetowe, o czym świadczyło udane włamanie na stronę Twittera. W tym samym czasie grupie udało się także zablokować chińską wyszukiwarkę Baidu. We wrześniu 2010 roku ICA zaatakowała natomiast znany blog technologiczny TechCrunch Europe, wykorzystując do tego zaawansowany zestaw narzędzi *Phoenix*. Wśród innych celów tej grupy należy wymienić przede wszystkim witryny wspieranej przez Zachód irańskiej opozycji, w tym m.in. finansowane przez Holandię Radio Zamaneh, a także uniwersytet Amirkabir. Dzięki tym działaniom grupa ta zyskała nawet miano „cyberbandytów Ahmedineżada"[61]. Można także wspomnieć o Turkish Cyber Army działającej pod silnym wpływem ideologii radykalnego islamu. Z jednej strony angażuje się ona w bieżące wydarzenia polityczne na Bliskim Wschodzie, m.in. regularnie atakuje strony izraelskie w związku z obroną interesów Palestyńczyków, a ponadto po przewrocie wojskowym w Egipcie aktywnie wsparła Bractwo Muzułmańskie. Z drugiej strony TCA działa przeciwko zachodnim koncernom i korporacjom transnarodowym, których działalność godzi ich zdaniem w dobro Turcji[62].

Tego typu konflikty w cyberprzestrzeni mogą występować także w nieco innej konfiguracji, pomiędzy „haktywistami patriotycznymi" a ich innymi podmiotami pozapaństwowymi. W czerwcu 2011 roku grupa Anonymous rozpoczęła np. operację *Turkey*, która miała na celu wsparcie tureckich protestów przeciwko cenzurze Internetu. W wyniku tej akcji strony rządu w Ankarze przez kilka dni były blokowane za pomocą metody DDoS. Co ciekawe, działania te spotkały się z reakcją patriotycznie motywowanych programistów z grupy Akincilar, którzy w ramach odwetu dokonali udanego włamania na stronę domową AnonPlus. Podobne środki przeciwko Anonymous podjęli haktywiści syryjscy z Syrian Cyber Army, ze względu na wojnę domową w tym kraju atakowano bowiem strony reżimu Baszara al Assada. W ramach zorganizowanej odpowiedzi zwolenników dyktatora zablokowano stronę domową tej grupy[63]. W trakcie konfliktu zbrojnego w Syrii pojawiła się również inna,

---

[61] Liedel, Piasecka, 2011: 20; A. Raff: *The „Iranian Cyber Army" Strikes Back*. Seculert, 24.10.2010: www.seculert.com/blog/2010/10/iranian-cyber-army-strikes-back.html; dostęp: 12.10.2013; *Who are the „Iranian Cyber Army"?* The Green Voice of Freedom, 19.02.2010: http://en.irangreenvoice.com/article/2010/feb/19/1236; dostęp: 12.10.2013.

[62] Zob. *Turkish Cyber Army*. Facebook: www.facebook.com/TurkeyCyberArmy; dostęp: 12.10.2013.

[63] K. Hannaford: *Hackers Hacked the Hackers' AnonPlus Social Network*. Gizmodo.com: http://gizmodo.com/5823351/hackers-hacked-the-hackers-anonplus-social-network; dostęp: 2.09.2013; *Syrian Cyber Army Hack Anonymous Hacking Group Website Leaving Message is this Cyber Warfare!* Allvoices.com: www.allvoices.com/contributed-news/10445808/video/87019121-syrian-cyber-army-hack-anonymous-hacking-group-website-leaving-message-is-this-cyber; dostęp: 2.09.2013.

zdecydowanie sławniejsza grupa — Syrian Electronic Army, której członkowie ogłosili, że celem jej powołania było przeciwdziałanie zmasowanej kampanii propagandowej wymierzonej w syryjski rząd. W ramach realizacji tego postulatu SEA z sukcesem włamała się m.in. na strony: Harvard University, „The Washington Post", „The Telegraph", „The Independent", Al Jazeery, Human Rights Watch czy BBC. Jednym z najgłośniejszych aktów tej grupy była podmiana zawartości witryny U.S. Marine Corps, gdzie opublikowano zdjęcia amerykańskich żołnierzy nie zgadzających się na udział w interwencji USA przeciwko reżimowi al Assada. Ta szeroko zakrojona kampania udowodniła, iż haktywizm patriotyczny staje się zjawiskiem coraz powszechniejszym[64]. Na koniec warto również wspomnieć, iż według opinii części ekspertów tego typu charakter miały wydarzenia w Estonii w kwietniu 2007 roku, od lat pojawiają się bowiem głosy wskazujące na fakt, iż przynajmniej za częścią cyberataków stał wówczas nie Kreml, lecz grupy patriotycznie motywowanych haktywistów (Ruus, 2008: 1).

Mając na uwadze powyższe rozważania, można wskazać na kilka cech haktywizmu patriotycznego jako nieustrukturalizowanej formy zagrożeń teleinformatycznych. Przede wszystkim należy podkreślić, iż podobnie jak konwencjonalny haktywizm charakteryzuje się ona niskim stopniem zorganizowania. Wskazani przez Pageta „cyberwojownicy" zbierają się co prawda w grupy, grupy te jednak nie posiadają wewnętrznej hierarchii, struktur oraz sformalizowanych relacji wewnętrznych. Członkostwo w tzw. cyberarmiach opiera się na dwóch przesłankach: odpowiednich umiejętnościach informatycznych oraz właściwych motywacjach politycznych. Należy też podkreślić, iż różnią się oni od haktywistów odmienną specyfiką działania: ich ataki mają zdecydowanie bardziej inwazyjny charakter, opierają się głównie na metodach DDoS wymierzonych przeciwko witrynom internetowym, mogą jednak objąć również inne, groźniejsze techniki, ich celem jest bowiem nie tylko zwrócenie uwagi opinii publicznej na określony problem, lecz przede wszystkim wsparcie interesu własnego państwa lub narodu w trakcie konfliktu lub kryzysu politycznego. W związku z tym mogą się interesować np. elementami składającymi się na teleinformatyczną infrastrukturę krytyczną. Warto również zwrócić uwagę na specyficzne motywacje. Wspomniany François Paget (2012: 28—30) wskazywał, iż tzw. cyberwojowników cechuje szeroko pojęty fundamentalizm poglądów, co więcej: są to grupy, które funkcjonują głównie w państwach autorytarnych. Podejście to budzi jednak pewne wątpliwości. Co prawda funkcjonują zespoły haktywistów, które rzeczywiście działają w oparciu o radykalne ideologie, nie stanowią one jednak głównego nurtu

[64] O. Katerji: *The Syrian Electronic Army Hacked the BBC*: www.vice.com/en_uk/read/the-syrian-electronic-army-hacked-the-bbc; dostęp: 2.09.2013; *Marine Corps responds to Syria-based cyber attack*. Marine Times, 09.09.2013: www.marinecorpstimes.com/article/20130909/NEWS/309090022/Marine-Corps-responds-Syria-based-cyber-attack; dostęp: 12.10.2013.

w tym środowisku, tego typu programiści działają bowiem w państwach, które są w pełni demokratyczne, a ich postawy wynikają z pobudek czysto patriotycznych. Ich aktywność w cyberprzestrzeni polega na obronie interesów własnego państwa i narodu lub ich promocji za pomocą cyberataków. Reasumując, haktywizm patriotyczny należy więc uznać za zdecydowanie poważniejsze zagrożenie bezpieczeństwa państw niż haking oraz konwencjonalny haktywizm (Lakomy, 2013e: 117—120).

3.3.1.4. Cyberprzestępczość

Badając zjawisko cyberprzestępczości pod względem zagrożeń dla bezpieczeństwa państw, należy zwrócić uwagę na fakt, iż jest to wyzwanie o charakterze globalnym, co szczególnie mocno podkreśla w ostatnich latach Organizacja Narodów Zjednoczonych. O jego skali mogą najlepiej świadczyć statystyki. Przede wszystkim, jak wspomniano wcześniej, globalny koszt cyberprzestępczości w 2012 roku wynosił ok. 100 mld dolarów. Miliony internautów na całym świecie każdego roku padają ofiarą różnorodnych akcji przeprowadzanych przez kryminalistów, najwięcej w Stanach Zjednoczonych, Chinach, Indiach, Niemczech oraz Brazylii. Na ich aktywność składają się m.in. włamania do poczty elektronicznej, kont bankowych, kradzież tożsamości, nieuprawnione wykorzystanie kart kredytowych czy włamania na portale społecznościowe. Doszło wręcz do wykształcenia się czarnego rynku przestępczych usług online, czego przejawem jest m.in. tworzenie, wykorzystanie i zarządzanie sieciami *botnet*, tworzenie i upowszechnianie złośliwego oprogramowania, zdobywanie wrażliwych danych osobowych czy informacji gospodarczych. Według badań ONZ w zależności od kraju między 1 a 17% osób korzystających z Internetu padło ofiarą cyberprzestępców. Dla porównania tradycyjna działalność kryminalna dotyka średnio ok. 5% populacji. O skali rozwoju tego procederu świadczy także fakt, iż w latach 2005—2012 liczba incydentów związanych z przestępstwami komputerowymi wzrosła aż o 600%. W 2012 roku średnie straty na osobę w różnych państwach wynosiły między 50 a 810 dolarów[65]. Według badań przeprowadzonych przez Rossa Andersona, Christa Bartona, Rainera Böhmego, Richarda Claytona, Michela J.G. van Eetena, Michaela Leviego, Tylera Moore'a oraz Stefana Savage'a w 2012 roku cyberprzestępcy na samych tylko oszustwach komputerowych zarobili ponad miliard

[65] Zob. *Comprehensive Study on Cybercrime*, 2013; *Cyber Crime Statistics and Trends*. Go-Gulf, 17.05.2013: www.go-gulf.com/blog/cyber-crime; dostęp: 4.09.2013; *Understanding Cybercrime*, 2012, s. 15.

dolarów. W latach 2008—2010 z tytułu tworzenia fałszywych programów antywirusowych uzyskali kolejne 97 mln dolarów. Zgodnie z ujawnionymi przez FBI danymi włamania na korporacyjne konta bankowe we wrześniu 2011 roku oznaczały straty na poziomie ok. 85 mln dolarów, w 2007 roku natomiast między 280 000 a 560 000 osób padło ofiarą udanych ataków na swoje konta bankowe online[66].

Na tle powyższych statystyk powstaje jednak pytanie, jak należy rozumieć proceder cyberprzestępczości. Zgodnie z ustawodawstwem większości państw świata każdy nieautoryzowany dostęp do danych w formie cyfrowej lub próba manipulacji nimi jest przestępstwem. Z tego punktu widzenia zarówno haking, haktywizm, cyberterroryzm, jak i cyberszpiegostwo są formami działalności kryminalnej (zob. Finklea, Theohary, 2012). Podobnie ogólnikowych sformułowań użyto w *Polityce Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej* (2013: 6), w której zauważono, iż jest to „czyn zabroniony w obszarze cyberprzestrzeni". Szanghajska Organizacja Współpracy zdefiniowała to pojęcie jako „wykorzystanie zasobów informacyjnych i/lub wpływ na nie w sferze informacyjnej w nielegalnych celach" (*Comprehensive Study*, 2013: 12—13). Brytyjska Wspólnota Narodów uznała ją za „akt przestępczy, którego celem jest informacja komputerowa" (Ibidem, s. 12—13). Z kolei w raporcie Międzynarodowego Związku Telekomunikacyjnego zauważono, iż jest to działalność, w której „komputery lub sieci są narzędziem, celem bądź miejscem aktywności kryminalnej" (*Understanding Cybercrime*, 2012: 11). Można również wspomnieć o definicji przyjętej przez *Konwencję Rady Europy o cyberprzestępczości* z 2001 roku, która stwierdziła, iż w skład tego procederu zaliczają się cztery grupy działań przy pomocy komputerów: naruszenia bezpieczeństwa, oszustwa i fałszerstwa, rozpowszechnianie pornografii dziecięcej oraz naruszenia praw autorskich. Problem ten podejmowany był i w polskiej literaturze specjalistycznej. Krzysztof J. Jakubski uznał przestępczość komputerową za „zjawisko kryminologiczne obejmujące wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informacje, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawo do programu komputerowego" (cyt. za: Siwicki, 2013: 11). Organizacja Narodów Zjednoczonych wyróżniła natomiast trzy grupy przestępstw komputerowych:

[66] R. Anderson, C. Barton, R. Böhme, R. Clayton, M.J.G. van Eeten, M. Levi, T. Moore, S. Savage: *Measuring the Cost of Cybercrime*. Workshop on the Economics of Information Security, WEIS 2012, 25—26.06.2012 Berlin: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf; dostęp: 4.09.2012; *The Cost of Cyber Crime*. Bloomberg Businessweek, 02.08.2012: www.businessweek.com/articles/2012-08-02/the-cost-of-cyber-crime; dostęp: 4.09.2013.

- akty przeciwko poufności, integralności i dostępności systemów lub danych komputerowych (np. nielegalny dostęp do komputerów, nielegalne przejęcie jego danych, produkcja złośliwego oprogramowania),
- akty komputerowe zmierzające do wyrządzenia szkody finansowej lub uzyskania określonych korzyści materialnych (oszustwa, kradzieże tożsamości, łamanie praw autorskich, rozsyłanie spamu),
- akty związane z zawartością danych w cyberprzestrzeni (mowa nienawiści, pornografia dziecięca czy wspieranie terroryzmu) (*Comprehensive Study*, 2013: 16).

Przyjęcie tak szerokiej definicji cyberprzestępczości w zasadniczym stopniu zaburzyłoby jednak optykę zagrożeń teleinformatycznych, jak wspomniano bowiem wcześniej, różnią się one diametralnie pod względem motywacji, stopnia organizacji czy wykorzystywanych metod. Na tym tle w analizie prowadzonej na gruncie nauk politycznych tak szerokie ujęcie byłoby zbyt ogólne i zaciemniałoby wielopłaszczyznowy, wielowymiarowy i dynamiczny obraz tych wyzwań. Utrudniłoby ponadto wypracowanie odpowiednich mechanizmów praktycznego reagowania na nie na poziomie państwowym, wskazywałoby bowiem, iż każdy cyberatak powinien spotkać się z reakcją właściwych organów ścigania, które są odpowiedzialne za walkę z przestępczością. Tym samym nawet najpoważniejsze z ataków, noszące znamiona operacji wojskowej wymierzonej np. w infrastrukturę krytyczną, nie mogłyby się spotkać z reakcją sił zbrojnych lub adekwatnymi działaniami w środowisku międzynarodowym. Zaprezentowane wyżej podejście *sensu largo*, jakkolwiek właściwe z perspektywy prawnej, należałoby zatem w prowadzonych rozważaniach zawęzić, tak aby odróżnić główny nurt przestępczości komputerowej od innych, jakościowo odmiennych zagrożeń teleinformatycznych (Lakomy, 2013d: 121).

Aby tego dokonać, warto wyjść od spojrzenia na historię tego procederu. Jak wspomniano, haking w swojej pierwotnej formie charakteryzował się dużym naciskiem na działania etyczne oraz samodoskonalenie. Z tego środowiska w latach 80. XX wieku zaczęły się jednak wyodrębniać jednostki i grupy, które chciały wykorzystać swoje wyjątkowe zdolności dla indywidualnego zysku. Tak ujmowana przestępczość komputerowa oznaczała więc proceder polegający na dokonywaniu cyberataków w celu osiągnięcia określonych korzyści materialnych. Składa się ona z trzech elementów: czynu zabronionego, świadomości, że prawo jest łamane, oraz społecznej szkodliwości, która jest wyższa niż znikoma (Ziomka, 2008: 12—13). Kluczowym aspektem tak rozumianej przestępczości komputerowej jest więc chęć osiągnięcia indywidualnych lub grupowych profitów, innych niż promocja określonego światopoglądu bądź rozwój własnych umiejętności, zawierałyby się w niej zatem wszelkie incydenty przeprowadzone przez dążących do uzyskania korzyści materialnych kryminalistów. Tego typu ujęcie pomijałoby natomiast szerokie spektrum amatorów, wandali, frustratów,

tzw. *script kiddies*[67], którzy jakkolwiek są przestępcami, to nie stanowią większego zagrożenia z perspektywy interesu społecznego.

Cyberprzestępczość w przyjętym, wąskim rozumieniu może więc w praktyce przybierać rozmaite formy. Za jej przejaw uznaje się dążenie do uzyskania wrażliwych informacji, które mogą zostać z zyskiem odsprzedane na czarnym rynku zarówno przez jednostki, jak i przez zorganizowane grupy przestępcze. Z jednej strony mogą być to więc prywatne dane, takie jak nazwy użytkownika i hasła do różnorodnych usług sieciowych (e-mail, e-bankowość), z drugiej natomiast przejawem tego procederu są też wszelkie włamania, których celem jest własność intelektualna: zdjęcia, muzyka, filmy, opracowania naukowe czy nawet zaawansowane technologie. Co więcej: cyberprzestępcy coraz częściej podejmują próby zdobywania informacji, które są później przydatne do szantażu i wyłudzania pieniędzy. Istnieje także stale rosnąca lista innych sposobów uzyskiwania korzyści materialnych związanych z wymuszaniem określonych zachowań u internautów. Może o tym świadczyć popularność omówionych już programów typu *ransomware*. Coraz częściej w ten sposób wykorzystywane są również kontrolowane przez przestępców sieci *botnet*, które można wynająć m.in. do rozsyłania spamu, złośliwego oprogramowania bądź do ataków na wybrane strony internetowe. Na tej podstawie należy stwierdzić, iż kryminaliści działający w cyberprzestrzeni stosują w zasadzie wszystkie dostępne metody cyberataków, obejmujące przede wszystkim narzędzia i techniki przydatne do wykradania informacji z komputerów, w tym np. *keyloggery*, *phishing* oraz trojany. Coraz częściej ponadto stosuje się bardziej inwazyjne sposoby, w tym sieci *botnet* oraz ataki typu DoS/DDoS, które mogą służyć m.in. do wymuszania haraczy[68].

Warto podkreślić, iż cyberprzestępczość jest zagrożeniem o zróżnicowanym poziomie zorganizowania, oprócz rzeszy pojedynczych kryminalistów coraz częściej przestrzeń teleinformatyczna jest bowiem wykorzystywana przez całe ich grupy lub w niektórych przypadkach także przez organizacje przestępcze działające dotychczas offline. Grupy cyberprzestępców z reguły mają podobne cechy jak organizacje hakerów i haktywistów: nie mają wyraźnie wyodrębnionej hierarchii, a stosunki między ich członkami mają charakter niesformalizowany. Zdecydowanie odmienne cechy mają natomiast zorganizowane grupy przestępcze, które współcześnie coraz częściej interesują się potencjałem sieci. Nie są one z reguły zainteresowane dokonywaniem głośnych cyberataków, które ściągnęłyby na nie uwagę organów ścigania, wykorzystują Internet i najnowsze technologie teleinformatyczne raczej w celu podniesienia swojej skuteczności na tradycyjnych obszarach działań, ICT są więc dla nich przydatne jako narzędzie

[67] Grupę tę wyróżnili m.in. Piotr Sienkiewicz i Halina Świeboda (2009: 90).

[68] Zob. Esquibel, Laurenzano, Xiao, Zuvich, 2005; P. Gontarczyk: *Cyberprzestępcy opracowują nowe metody szkodliwych ataków*. PCLab, 07.07.2008: http://pclab.pl/news33122.html; dostęp: 4.09.2013. Za: Lakomy, 2013d: 121—122.

komunikacji z innymi organizacjami przestępczymi, promocji i sprzedaży narkotyków bądź „prania brudnych pieniędzy”[69].

Fenomen ten w zdecydowanej większości przypadków nie wiąże się z żadnymi poważniejszymi reperkusjami dla stosunków międzynarodowych. Akty zagranicznej cyberprzestępczości prowadzą z reguły do zastosowania mechanizmów współpracy państwowych wymiarów sprawiedliwości[70]. Konsekwencje polityczno-prawne tego typu procederu na arenie międzynarodowej mogłyby wystąpić tylko w sytuacji, w której państwo będące źródłem masowych cyberataków nie starałoby się im zapobiec oraz nie współpracowałoby z ich ofiarami w celu ukarania sprawców. Wówczas zgodnie z prawem międzynarodowym publicznym zaistniałaby odpowiedzialność pośrednia tego kraju za bezprawne działania osób prywatnych wskutek „zachęcania i tolerowania tego rodzaju działań, niezastosowania przez państwo środków prewencyjnych lub nieukarania sprawców bezprawnych działań” (Bierzanek, Symonides, 2002: 154). Taka sytuacja w ostatnich latach miała miejsce w relacjach amerykańsko-chińskich, kiedy kolejne cyberataki pochodzące z terytorium ChRL nie spotkały się z należytą reakcją Pekinu, co doprowadziło w konsekwencji do protestów amerykańskiego rządu[71].

Reasumując, warto odwołać się do słów Marcina Terlikowskiego (2009: 96), który zauważył, iż komputerowi kryminaliści „nie mają zazwyczaj interesu w bezpośrednim uderzeniu w podmioty państwowe, gdyż mogłoby to zwrócić uwagę władz i w konsekwencji skutkować wobec nich podjęciem działań przez organy ścigania”. Z jednej strony cyberprzestępczość stanowi więc raczej pośrednie zagrożenie dla bezpieczeństwa narodowego i międzynarodowego. Jednostki i grupy zajmujące się tym procederem niezwykle rzadko biorą na cel elementy systemu obronnego lub infrastruktury krytycznej kraju. Z drugiej jednak strony współczesna skala cyberprzestępczości sprawia, iż mimo wszystko może ona negatywnie wpływać m.in. na rozwój gospodarczy czy funkcjonowanie administracji publicznej. Częstotliwość cyberataków o podłożu kryminalnym może także spowolnić proces rozwoju naukowo-technicznego, zniechęcając użytkowników do kolejnych osiągnięć rewolucji informatycznej.

---

[69] Zob. P. Williams: *Organized Crime and Cyber-Crime: Implications for Business*. CERT Coordination Center: *www.cert.org/archive/pdf/cybercrime-business.pdf*; dostęp: 4.09.2013; *Prospective Analysis*, 2010; Maurer, 2011, s. 37—38.

[70] Szczególnie interesująca na tym tle jest działalność Interpolu. Zob. *Cybercrime*. Interpol: www.interpol.int/Crime-areas/Cybercrime/Cybercrime; dostęp: 7.10.2013.

[71] *Hillary Clinton calls on China to probe Google attack*. BBC NEWS, 21.01.2010: http://news.bbc.co.uk/2/hi/8472683.stm; dostęp: 4.09.2013.

3.3.2. Zagrożenia ustrukturalizowane

3.3.2.1. Cyberterroryzm

Jak wspomniano wyżej, w debacie publicznej poświęconej problematyce bezpieczeństwa teleinformatycznego jednym z częściej stosowanych terminów jest *cyberterroryzm*. Szczególnie w mediach masowych stosuje się go do określenia wydarzeń, które częstokroć nie mają większego związku z istotą tego zjawiska. Od lat toczy się również dyskusja naukowa dotycząca tego, czy termin *cyberterroryzm* jest w ogóle zasadny. Jest to tym bardziej widoczne, iż definicja samego *terroryzmu* również rodzi poważne spory w środowisku naukowym[72]. Aby oddać kontrowersje związane z tym zagadnieniem, warto ponownie odwołać się do rozważań Krzysztofa Liderman. Zarzucając badaczom nadmierne stosowanie pojęć z przedrostkiem *cyber-*, zadał on interesujące pytanie:

> Dlaczego nie używać istniejącego już w naszym prawie terminu *terroryzm*? […] Zakładając roboczo, bo powszechnie uznanej definicji nie ma, że *cyberterroryzm* to terroryzm prowadzony w cyberprzestrzeni (cokolwiek miałoby to znaczyć), można zapytać, czy terrorystów działających na pokładach samolotów zaczniemy nazywać „aeroterrorystami" (Liderman, 2012: 60—65).

Jest to zarzut, który stosunkowo łatwo obalić. Porwania samolotów, działania znane z 11 września 2001 roku, zamachy bombowe i inne akcje podejmowane przez organizacje terrorystyczne mają charakter *stricte* materialny. W przeciwieństwie do nich cyberterroryzm wiąże się z aktywnością w przestrzeni teleinformatycznej, która rządzi się innymi prawami niż pozostałe przestrzenie konwencjonalne (lądowa, morska, powietrzna, kosmiczna). Również jego skutki mają z reguły zupełnie inny charakter. To właśnie ze względu na to kategoria owa weszła na stałe do systemów prawnych państw na całym świecie, wykorzystanie nowego terminu dla określenia jakościowo odmiennej formy terroryzmu wydaje się zatem jak najbardziej uprawnione, choć nie ułatwia dokładnego zdefiniowania tego pojęcia.

W literaturze specjalistycznej pojawiło się w ostatnich kilkunastu latach szereg propozycji w tym zakresie. Po raz pierwszy terminu tego użył Barry Collin już w latach 80. XX wieku, w dyskursie naukowym zaistniał on jed-

[72] Zob. Noor, 2011, nr 2; Gordon, 2008; Wilson, 2003; Nelson, Choi, Iacobucci, Mitchell, Gagnon, 1998; Robinson, 2012; Yagil, 2002.

nak zdecydowanie później[73]. Według klasycznej definicji Dorothy E. Denning (2000) jest to „konwergencja terroryzmu i cyberprzestrzeni". Według autorki warunkiem uznania cyberataku za akt terrorystyczny powinien być jego skutek, wiążący się z przemocą przeciwko osobom lub mieniu bądź z pojawieniem się strachu. Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell oraz Greg Gagnon (1998: 9) uznali, iż jest to „bezprawne zniszczenie lub zakłócenie cyfrowej własności zmierzające do zastraszenia lub zmuszenia rządów bądź społeczeństw dla realizacji celów o charakterze politycznym religijnym czy ideologicznym". Zdaniem Jamesa A. Lewisa (2002) zjawisko to obejmuje „wykorzystanie sieci komputerowych jako narzędzia paraliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań". Center for Strategic and International Studies scharakteryzowało ten termin jako „wykorzystanie narzędzi sieci komputerowych do wyłączania [elementów — M.L.] narodowych infrastruktur krytycznych (np. energii, transportu, działań rządowych) lub zmuszenia bądź zastraszenia rządu lub społeczeństwa" (za: Tafoya, 2011). Ron Dick uznał go za „akt kryminalny popełniony za pomocą komputerów, którego rezultatem jest przemoc, śmierć i/lub zniszczenie oraz pojawienie się terroru w celu wymuszenia na rządzie zmian jego polityki" (za: Mehan, 2008: 32). David S. Wall (2007: 221) wskazał, iż jest to „wykorzystanie komputerów do ataku na fizyczną infrastrukturę w celu masowego generowania strachu i niepewności oraz, w teorii, manipulowania agendą polityczną". Inne stanowisko zajął Martin C. Libicki (2007: 46), który stwierdził, iż terroryści wykorzystują Internet do trzech rodzajów działań: rekrutacji, dystrybucji materiałów instruktażowych oraz sprawowania bezpośredniego dowodzenia i kontroli (*command & control*).

Interesujące propozycje opracowało również polskie środowisko naukowe. Marcin Terlikowski (2009: 111) uznał cyberterroryzm za „działalność terrorystyczną, w której programy i urządzenia elektroniczne oraz systemy teleinformatyczne spełniają funkcję specyficznego rodzaju narzędzia — broni w rękach terrorystów". Tomasz Trejderowski (2013: 172) wskazał, iż jest to „połączenie sieci i terroryzmu; mogą to być zarówno ataki grup terrorystycznych przeprowadzane w Internecie — cyberataki na serwery i strony internetowe powodujące poważne straty finansowe — jak i wykorzystanie sieci do wsparcia lub przeprowadzenia ataków terrorystycznych w świecie rzeczywistym". Z kolei Tomasz Szubrycht (2005: 176) zauważył w tej dziedzinie ciekawą prawidło-

[73] J. Brickey: *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*. Combating Terrorism Center, 23.08.2012: www.ctc.usma.edu/posts/defining-cyber terrorism-capturing-a-broad-range-of-activities-in-cyberspace; dostęp: 6.09.2013.

wość, stwierdził bowiem, iż większość definicji cyberterroryzmu zawiera się w dwóch odrębnych tendencjach. Zgodnie z pierwszą szczególny nacisk kładzie się na możliwość wykorzystania sieci komputerowych do przeprowadzania ataków. Zgodnie z drugą to komputery oraz ich sieci stanowią cel działań terrorystów. Wydaje się, iż obie te tendencje są zasadne i razem składają się na pełen obraz tego zjawiska.

Jedne z najciekawszych definicji cyberterroryzmu w rodzimej literaturze specjalistycznej zaproponowali Marcin F. Gawrycki, Agnieszka Bógdał-Brzezińska oraz Ernest Lichocki. Zgodnie z podejściem dwóch pierwszych autorów jest to „politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów". W szerszym ujęciu jest to również „wykorzystanie Internetu przez organizacje terrorystyczne do komunikowania się, propagandy i dezinformacji" (Gawrycki, Bógdał-Brzezińska, 2003: 73). Według Ernesta Lichockiego cyberterroryzm to „przemyślany politycznie lub militarnie motywowany atak albo groźba ataku na systemy teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia Infrastruktury Krytycznej Państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno-militarnych działań. Cyberatak może być przeprowadzony jako część składowa większej polityczno-militarnej akcji lub samodzielnego ataku". Podobnie jak Marcin F. Gawrycki i Agnieszka Bógdał-Brzezińska uznał on, iż zjawisko to obejmuje również propagandę, rekrutację, komunikację, mobilizację, zbieranie informacji o potencjalnych celach, planowanie, koordynację akcji, dezinformację i walkę psychologiczną w cyberprzestrzeni realizowane przez organizacje terrorystyczne (Lichocki, 2011: 71; za: Lakomy, 2013d: 124—126).

Oprócz środowiska naukowego próby zdefiniowania tego procederu podejmują rządy poszczególnych państw oraz organizacje międzynarodowe. Wśród wielu z nich uwagę zwraca raport United Nations Office on Drugs and Crime, który zaliczył do cyberterroryzmu następujące działania w sieci: propagandę (w tym np. rekrutację, inspirowanie ideologią), finansowanie terroryzmu, szkolenia, planowanie, wykorzystanie Internetu do ataków terrorystycznych oraz same cyberataki (*The Use of Internet*, 2012: 3—12).

Z kolei amerykańskie National Infrastructure Protection Center uznało cyberterroryzm za „akt kryminalny popełniony za pomocą komputerów w celu zmuszenia rządu do zmiany swej polityki, którego skutkiem jest przemoc, śmierć i/lub zniszczenia oraz strach" (za: Wilson, 2003: 4). W polskiej *Polityce Ochrony Cyberprzestrzeni RP* z 2013 roku (s. 6) ujęto to zagadnienie bardzo ogólnie, jako „przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni".

Wydaje się, iż najbardziej trafne definicje tego zagrożenia sformułowali Marcin Florian Gawrycki, Agnieszka Bógdał-Brzezińska oraz Ernest Lichocki. Z jednej strony objęły one sam fakt dokonania cyberataku, jego cele, jak

i specyficzne motywacje. Z drugiej strony w obu przypadkach dostrzeżono propagandowo-informacyjną działalność organizacji terrorystycznych, które zaczęły wykorzystywać sieci komputerowe do promocji własnego radykalnego światopoglądu, zdobywania zwolenników, organizowania zamachów oraz komunikacji z innymi, podobnymi ideowo grupami. W tym kontekście za akt cyberterroryzmu należałoby uznać przede wszystkim każdy motywowany politycznie cyberatak, który jest wymierzony w systemy teleinformatyczne, znajdujące się na nich dane oraz związane z nimi usługi i urządzenia. Bezpośrednim celem tego aktu jest dokonanie znacznych materialnych lub niematerialnych szkód, które mają wpływ na funkcjonowanie państwa lub społeczeństwa. Pośrednio powinien on zmierzać do wymuszenia zmiany polityki rządu, a szerzej: nastawienia elit politycznych oraz wyborców. Z aktem cyberterroryzmu wiąże się więc powstanie zjawiska strachu. W szerszym rozumieniu na proceder ten składają się również inne, wymienione już wyżej działania organizacji terrorystycznych w Internecie.

Na tej podstawie można wskazać na kilka przykładów działań cyberterrorystycznych na początku XXI wieku. Przede wszystkim warto wspomnieć o wydarzeniach, które miały miejsce w Brazylii w latach 2005 i 2007. Wówczas, jak podaje część źródeł, doszło do masowej awarii sieci elektroenergetycznej, która nastąpiła w wyniku domniemanych włamań komputerowych. Ich skutkiem było pozbawienie prądu ok. 60 milionów Brazylijczyków. Ze względu na skąpe i czasami sprzeczne dane na ten temat sklasyfikowanie tych incydentów jako cyberterroryzmu nie jest jednak przesądzone[74]. W wymiarze międzypaństwowym za przykład może służyć *casus* robaka *Stuxnet*, którego celem było sabotowanie irańskich wirówek wzbogacających uran. Jego zastosowanie godziło w infrastrukturę krytyczną reżimu ajatollahów oraz charakteryzowało się wyraźną intencją polityczną (zob. *Annual Report PandaLabs*, 2010; Matrosov, Rodionov, Harley, Malcho, 2010). Warto również zwrócić uwagę na coraz intensywniejszą działalność propagandowo-informacyjną organizacji terrorystycznych w sieci[75]. Grupy radykalne, szczególnie islamskie, dostrzegły na przełomie XX i XXI wieku użyteczność Internetu do promowania własnej ideologii wśród rzeszy jego użytkowników, a przez to inspirowania ich do kolejnych aktów terrorystycznych. W 1998 roku 12 z 30 organizacji terrorystycznych z listy Departamentu Stanu USA prowadziło strony internetowe, na których zamieszczało informacje o swojej aktywności. W 2004 roku niemal wszystkie odwoływały się do tego typu narzędzi, w tym m.in. PKK, Hamas oraz Hez-

[74] M. Mylrea: *Brazil's Next Battlefield: Cyberspace*. „Foreign Policy Journal" 15.11.2009: www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace; dostęp: 6.09.2013.

[75] Warto podkreślić, iż Internet odegrał istotną rolę w przygotowywaniu zamachów w Nowym Jorku i Waszyngtonie. Jeden z pomysłodawców tej operacji, Khalid Shaikh Mohammed, komunikował się online z przynajmniej dwoma sprawcami ataków na WTC. Zob. Wilson, 2008, s. 19.

bollah (*Understanding Cybercrime*, 2012: s. 35). Wśród ciekawych przykładów należy wymienić portal czeczeńskich islamistów kavkazcenter.com, gdzie prezentowane są materiały propagandowe dotyczące konfliktu z Rosją na Kaukazie[76]. Podobną rolę w stosunku do Al Kaidy pełniła założona w 2004 roku strona Shumukh al-Islam, która była wykorzystywana przez organizację do publikowania przemówień przywódców. Była ona wraz z innymi, mniej popularnymi stronami, takimi jak Ansar al-Mujahideen Arabic Forum, jednym z podstawowych miejsc wymiany poglądów i informacji między dżihadystami (Nakashima, Warrick, 2012). O rosnącym zainteresowaniu terrorystów tą domeną świadczą również informacje, według których takie grupy, jak Lashkar e-Tayyibah czy iracka Al Kaida od lat rozwijają umiejętności informatyczne swoich wybranych członków. W tym kontekście Ayman al Zawahiri miał wręcz doradzać zabitemu przywódcy Al Kaidy w Iraku, Abu Musabowi al Zarqawi, iż połowa „bitwy o islam" powinna być prowadzona w Internecie (Brennan, 2012: 3). Można również wspomnieć o anglojęzycznym islamskim czasopiśmie „Inspire", którego zadaniem było, jak sama nazwa wskazywała, inspirowanie młodych czytelników, głównie Brytyjczyków i Amerykanów, do prowadzenia wojny religijnej z „niewiernymi"[77].

Mając na uwadze powyższe rozważania, należałoby więc wyróżnić kilka najbardziej istotnych cech cyberterroryzmu jako zagrożenia dla bezpieczeństwa teleinformatycznego. Przede wszystkim, podobnie jak konwencjonalny terroryzm, może to być działalność prowadzona zarówno przez posiadające podmiotowość prawną państwa, jak i grupy niepaństwowe, w tym organizacje terrorystyczne, powstańców czy inne radykalnie usposobione ruchy działające w oparciu o określoną ideologię. W odróżnieniu od haktywizmu czy hakingu cyberterroryzm ma zatem zasadniczy wpływ na bezpieczeństwo narodowe i międzynarodowe. Dokonywane w ten sposób ataki teleinformatyczne w dużej mierze mogą się wiązać z poważnymi reperkusjami w środowisku międzynarodowym. Należy także zauważyć, iż jest to zagrożenie charakteryzujące się wysokim stopniem zorganizowania sprawców. Struktura organizacyjna instytucji państwowych, które mogą być za te akty odpowiedzialne, jest naturalnie w pełni sformalizowana, posiada wyraźnie wyodrębnioną hierarchię, strukturę oraz cele. W przypadku organizacji niepaństwowych mimo występowania więzi niesformalizowanych stopień zorganizowania jest również wysoki, z reguły występuje bowiem hierarchia oraz komórki realizujące ściśle wyznaczone zadania[78]. Zresztą same operacje cyberterrorystyczne wymagają znacznych przygotowań, wiedzy i umiejętności, wyraźnego podziału obowiązków oraz jasno określonego

[76] http://kavkazcenter.com; dostęp: 6.09.2013.

[77] Ibidem, s. 4. Szerzej na temat cyberdżihadyzmu w: Kosmynka, 2013: 99—123.

[78] Zob. T. Hashemi: *An Introduction to Terrorist Organisational Structures*. TheRiskyShift.com, 06.06.2012: http://theriskyshift.com/2012/06/an-introduction-to-terrorist-organisational-structures; dostęp: 9.12.2013.

sposobu działania dla osiągnięcia wyznaczonych celów. Należy ponadto podkreślić, iż motywacje czynów cyberterrorystycznych mają głównie charakter polityczny, religijny, a w pewnym sensie również wojskowy. Co prawda polityczne motywacje towarzyszą również haktywizmowi, mają one jednak zupełnie inny charakter, haktywiści działają bowiem, przynajmniej oficjalnie, w imię wyższych, uniwersalnych wartości, praw człowieka czy demokracji. Działalność cyberterrorystyczna wiąże się natomiast z nastawieniem na realizację interesów i pragnień wyłącznie zaangażowanej w nią grupy. Co więcej, jak zauważyła Dorothy E. Denning, oba zagrożenia różnią się także sposobem działania: podczas gdy haktywiści szukają jedynie rozgłosu, cyberterroryzm skierowany jest na wyrządzenie jak największych zniszczeń i szkód przeciwnikowi, ze stratami ludzkimi włącznie (za: Bógdał-Brzezińska, Gawrycki, 2003: 61). W tym kontekście należałoby podkreślić, iż cyberterroryzm może mieć skutki zarówno w wymiarze niematerialnym, jak i materialnym. W związku z tym, na co zwracał uwagę m.in. James A. Lewis, infrastrukturę krytyczną należy uznać za obszar szczególnego zainteresowania terrorystów działających w cyberprzestrzeni, biorąc ją na cel, mieliby bowiem szansę dokonania jak największych zniszczeń, które byłyby uciążliwe lub wręcz katastrofalne z punktu widzenia funkcjonowania państwa (zob. Bumiller, 2012; Lewis, 2002; Lakomy, 2013d: 125—127). Należałoby zwrócić uwagę także na właściwości techniczne działań cyberterrorystycznych. Dokonując ataków komputerowych, terroryści odwołują się głównie do metod najbardziej zaawansowanych i inwazyjnych. Nie tylko oznacza to wykorzystanie popularnego DDoS, ale także skomplikowanego, złośliwego oprogramowania oraz wcześniej niespotykanych technik włamań. Cyberterrorystom zazwyczaj nie przydają się natomiast metody stosowane zazwyczaj do działań szpiegowskich, wywiadowczych, takich jak np. *phishing*. Nadal spore wątpliwości budzą sposoby zwalczania cyberterroryzmu. Jak zauważył John W. Brennan (2012: 1—2), kinetyczne uderzenia przeciwko organizacjom terrorystycznym zgodnie z panującymi uregulowaniami prawnymi sprawiają z reguły zdecydowanie mniej problemów niż działania prowadzone w przestrzeni teleinformatycznej. Od lat toczy się zatem dyskusja, w jaki sposób należy przeciwdziałać cyberterroryzmowi, zarówno w wymiarze politycznym, wojskowym, jak i prawnym.

Reasumując, należy podkreślić, iż zjawisko cyberterroryzmu staje się stopniowo coraz poważniejszym zagrożeniem bezpieczeństwa teleinformatycznego. Podobnie jak konwencjonalny terroryzm jest to fenomen niezwykle dynamiczny, obejmujący zestaw politycznie, religijnie czy nawet wojskowo motywowanych działań, których celem jest nie tylko dokonanie poważnych szkód, lecz również wywarcie doniosłego efektu psychologicznego na społeczeństwie oraz elitach rządzących. Należy przy tym pamiętać, iż *sensu largo* cyberterroryzm obejmuje również cały zestaw innych, nieinwazyjnych działań o charakterze propagandowym, podejmowanych przez radykalne organizacje w Internecie. Jest to zjawi-

sko coraz powszechniejsze, szczególnie wobec rosnącego zainteresowania siecią ze strony kolejnych organizacji islamskich.

3.3.2.2. Cyberszpiegostwo

Za kolejne ustrukturalizowane zagrożenie teleinformatyczne należy uznać cyberszpiegostwo, które w ostatnich latach stało się niezwykle popularne. Mimo to w literaturze przedmiotu stosunkowo niewiele miejsca poświęca się próbom zdefiniowania tego procederu (zob. np. Even, Siman-Tov, 2012: 20—22). Najogólniej można go scharakteryzować jako dokonywanie cyberataków w celu zdobycia informacji niejawnych przez państwa i powiązane z nimi podmioty pozapaństwowe. Mając to na uwadze, warto na wstępie wskazać na powody wykształcenia się tego zjawiska. Przede wszystkim należy zauważyć, iż cyberprzestrzeń ze względu na jej omówione wcześniej cechy stała się bardzo dogodnym miejscem zbierania informacji. W przeciwieństwie do tradycyjnych form działalności wywiadowczej zastosowanie osiągnięć rewolucji informatycznej jest z reguły bezpieczniejsze oraz zdecydowanie tańsze, włamania komputerowe nie narażają bowiem agentów wywiadu na niebezpieczeństwo zatrzymania przez obce służby, a państwa unikają w ten sposób szeregu skomplikowanych działań w wymiarze organizacyjnym (np. stworzenia fałszywych dokumentów, zakupu specjalistycznych urządzeń, przerzutu osób itp.). Tendencje te wzmacnia dodatkowo rosnące znaczenie informacji we współczesnym świecie (zob. Liedel, 2011). Sprawia to, iż poszczególne podmioty pragną coraz szybciej uzyskiwać dane o fundamentalnym znaczeniu dla procesów politycznych, gospodarczych, społecznych czy, co naturalne, również militarnych. Stosowane od wieków tradycyjne sposoby nie są w stanie zaspokoić wszystkich tych potrzeb. W tej sytuacji wykorzystanie specyficznego środowiska, którym jest cyberprzestrzeń, może się jawić jako swoiste remedium, dodatkowe źródło wiadomości na temat tendencji i wydarzeń w środowisku międzynarodowym, choć należy podkreślić, iż cyberszpiegostwo nigdy nie będzie w stanie zastąpić działań wywiadowczych w terenie, a jedynie je uzupełniać (Lakomy, 2013d: 128).

Wydaje się, że to właśnie te przesłanki sprawiają, iż działalność wywiadowcza w cyberprzestrzeni od końca XX wieku stała się jedną z dominujących form zagrożeń teleinformatycznych. W ciągu ostatnich trzech dekad można było zaobserwować proces rosnącej liczby ataków komputerowych, których głównym celem było zdobycie danych o różnym stopniu poufności. Stosunkowo nieskomplikowane ataki z lat 80. dość szybko przekształciły się w wysoce zaawan-

sowane operacje, których celem stawały się nie tylko instytucje państwowe, ale także korporacje transnarodowe oraz ośrodki badawcze. Należy podkreślić, iż proceder, o którym mowa, jakościowo różnił się od podobnych, opisanych już działań cyberprzestępczych, w przeciwieństwie do nich cyberszpiegostwem zainteresowały się bowiem poszczególne rządy oraz powiązane z nimi grupy specjalistów. Od ataków o podłożu kryminalnym, których celem również może być uzyskanie wrażliwych danych, cyberszpiegostwo odróżniały nie tylko odmienne źródła, ale również motywacje, przede wszystkim o charakterze politycznym lub gospodarczym, ponieważ rządy poszczególnych państw dostrzegły rosnącą możliwość wykorzystania wykradzionych informacji zarówno w polityce wewnętrznej, jak i zagranicznej. Wiadomości o działaniach innych aktorów stosunków międzynarodowych mogą zostać np. wykorzystane, aby je wyprzedzić lub przygotować odpowiednią reakcję, w wymiarze gospodarczym zaś szczególnie istotne wydaje się wykradanie najnowszych technologii cywilnych i wojskowych, w czym od lat specjalizują się m.in. programiści chińscy[79]. Tego typu dane, wyprowadzone z komputerów ośrodków badawczych bądź wielkich korporacji, mogą zostać z korzyścią użyte przez rodzimy przemysł. Źródła działalności cyberszpiegowskiej mają więc charakter wysoce zorganizowany. Należy do nich zaliczyć przede wszystkim państwa, które dążą w ten sposób do maksymalizacji skuteczności swoich przedsięwzięć politycznych i gospodarczych.

Warto zauważyć, iż cyberataki o podłożu wywiadowczym mają unikalne właściwości z perspektywy stosowanych metod operacyjnych. Wykorzystuje się tu techniki, które polegają na uzyskaniu nielegalnego dostępu do danych w formie cyfrowej, nie alarmując jednocześnie ich właścicieli. Włamujący nie odwołują się więc do takich środków, jak DoS/DDoS, lecz funkcjonują w sposób zdecydowanie bardziej wyrafinowany. Często stosowaną metodą jest np. *phishing*, a szerzej: inżyniera społeczna. Podszywając się pod zaufaną osobę lub instytucję, specjaliści uzyskują wrażliwe informacje o funkcjonujących zabezpieczeniach lub zdobywają hasła i nazwy użytkownika do kont administracyjnych. Inną popularną metodą jest zainfekowanie komputera bądź sieci złośliwym oprogramowaniem (trojanem, robakiem), które umożliwia zdalne wyłączenie oprogramowania antywirusowego oraz przejęcie kontroli nad systemem.

W tym kontekście można przytoczyć wiele ciekawych przykładów, które dowodzą, iż cyberszpiegostwo jest coraz poważniejszą formą zagrożeń teleinformatycznych. Do pierwszych incydentów tego typu dochodziło, jak wspomniano, już w latach 80. XX wieku, jednak dopiero na przełomie XX i XXI wieku proceder ten osiągnął dojrzałą i groźną formę. W 1998 roku ujawniono w Stanach Zjednoczonych wspomnianą już aferę *Moonlight Maze*, w ramach której odkryto, iż z komputerów m.in. Pentagonu, NASA czy Departamentu Energii nielegalnie wyprowadzano tajne dane. Cyberataki pochodziły prawdopodobnie

[79] Zob. *Exposing One of China's*, 2012. Za: Lakomy, 2013d: 128.

z terytorium byłego Związku Radzieckiego[80]. W 2003 roku chińska grupa przeprowadziła operację określaną mianem *Titan Rain*, której celem były serwery rządu, największych korporacji oraz instytucji badawczych w Stanach Zjednoczonych. Zakończone sukcesem włamania pozwoliły wyprowadzić wrażliwe dane dotyczące m.in. technologii wykorzystywanych przez NASA, Lockheed-Martin oraz Redstone Arsenal (Graham, 2005; Lakomy, 2011b: 144—148). Do kolejnych głośnych incydentów cyberszpiegowskich doszło w 2007 roku, kiedy po raz kolejny chińscy programiści wzięli na cel Stany Zjednoczone: tym razem włamano się do komputerów Departamentów Stanu, Obrony i Handlu. Zdecydowanie groźniejsze w swej naturze były jednak cyberataki, które nastąpiły rok później: mimo odseparowania amerykańskich sieci wojskowych od cywilnego Internetu chińskim specjalistom udało się wyprowadzić z nich dane, wykorzystując przede wszystkim metody inżynierii społecznej[81]. Bardzo ciekawym przykładem było również ujawnienie przez zespół Rona Deiberta z „Information Warfare Monitor" chińskiej grupy cyberszpiegowskiej Gh0stNet. Stała ona za włamaniami komputerowymi w 103 krajach, w tym np. w Niemczech, Pakistanie, Tajlandii oraz na Cyprze. Według raportu 30% z nich skupiło się na „celach wysokiej wartości", w tym komputerach ambasad, ministerstw spraw zagranicznych, organizacji międzynarodowych, organizacji pozarządowych czy mediów. Co ciekawe, ofiarą ataków padli również tybetańscy opozycjoniści, których działania śledzono dzięki wykorzystaniu kamer internetowych (zob. Deibert, Rohozinski, 2009). W tym samym czasie amerykańskie media ujawniły, iż w trakcie wyborów prezydenckich w USA w 2008 roku senator John McCain był szpiegowany przez obce państwa za pomocą specjalistycznego oprogramowania zainstalowanego na komputerach jego współpracowników[82]. Można także przytoczyć ostrzeżenie MI5 z 2010 roku, według którego chiński wywiad wykorzystywał do nawiązywania kontaktów z brytyjskimi przedsiębiorcami zainfekowane złośliwym oprogramowaniem karty pamięci oraz kamery internetowe. Ich instalacja umożliwiała wywiadowi ChRL zdalny dostęp do komputera (Liedel, Piasecka, 2011: 19). Wszystkie wspomniane wyżej wydarzenia wywoływały, co zrozumiałe, poważne reperkusje polityczne. Miało to miejsce np. po atakach na korporację Google. Początkowo ich źródła utożsamiano z chińskimi grupami przestępczymi, które w ten sposób miały uzyskiwać znaczne korzyści materialne. W lutym 2013 roku korporacja Mandiant opublikowała jednak raport, w którym stwierdzono, iż za aktywnością cyberszpiegowską wymierzoną

[80] *Cyberwar — warnings*. PBS: www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings; dostęp: 13.10.2013.

[81] T. Greene: *Pentagon officials details U.S. military net attack*. 25.08.2010: www.networkworld.com/news/2010/082510-pentagon-net-hack.html; dostęp: 20.02.2013.

[82] *Five Serious Cases of Cyberespionage*. Fox News, 22.04.2009: www.foxnews.com/story/2009/04/22/five-serious-cases-cyberespionage; dostęp: 13.10.2013.

w USA stoi jednostka nr 61398 Chińskiej Armii Ludowo-Wyzwoleńczej[83]. Wpisało się to więc w szerszy kontekst amerykańsko-chińskiej rywalizacji na arenie międzynarodowej w ostatnich latach, świadcząc zarazem o tym, iż armia ChRL wyspecjalizowała się w wykradaniu informacji, które mogłyby posłużyć zrównoważeniu potęgi Stanów Zjednoczonych. W tym świetle Alexander Melnitzky (2012: 568—569) zastanawiał się wręcz, czy tego typu działania mogą stanowić podstawę zastosowania mechanizmów samoobrony lub wojny prewencyjnej.

Reasumując, trzeba wskazać, że cyberszpiegostwo stanowi współcześnie coraz częstszy proceder. Do cyberataków w celu zdobycia informacji niejawnych odwołują się już nie tylko Chiny, ale także szereg innych państw. Warto podkreślić, iż jakkolwiek same włamania nie wywołują bezpośrednich i poważnych szkód w oprogramowaniu lub kontrolowanych przez nie urządzeniach, to stanowią niezwykle poważne zagrożenie, ponieważ utrata wrażliwych danych dotyczących np. systemu obronnego, funkcjonowania infrastruktury krytycznej bądź najnowszych technologii może mieć katastrofalne skutki nie tylko dla pozycji międzynarodowej kraju czy jego konkurencyjności gospodarczej, ale także dla jego bezpieczeństwa (*Cyber Espionage*, 2011: 7).

3.3.2.3. Operacje zbrojne[84] w cyberprzestrzeni

Na tle powyższych cyberzagrożeń wraz z końcem zimnej wojny pojawiły się głosy wskazujące, iż przestrzeń teleinformatyczna może być wykorzystana także w charakterze piątego teatru wojny, obok ziemi, wody, powietrza i kosmosu. Sugerowałoby to, iż cyberprzestrzeń nie byłaby już jedynie domeną wykorzystywaną przez przestępców, hakerów czy terrorystów, lecz także armie poszczególnych państw. W styczniu 1996 roku zwrócił na to uwagę amerykański ośrodek badawczy RAND, który w ogłoszonym przez siebie raporcie stwierdził możliwość prowadzenia „strategicznej wojny w cyberprzestrzeni”[85]. Na tym etapie rewolucji informatycznej była to zaledwie wizja, która w przyszłości bynajmniej nie musiała się ziścić, wraz z postępującymi procesami komputeryzacji i informatyzacji stała się ona jednak stopniowo coraz bardziej realna. W tym kontekście

[83] *Secretary of State Hillary Clinton says China's Cyber Attacks Must Face Consequences*. Government Security: www.governmentsecurity.org/latest-security-news/secretary-of-state-hillary-clinton-says-chinas-cyber-attacks-must-face-consequences.html; dostęp: 9.09.2013; *Exposing One of China's, Communist Chinese Cyber-Attacks*, 2011. Za: Lakomy, 2014: 128—130.

[84] Przez operację zbrojną można rozumieć *sensu largo* jako zestaw działań wojskowych zmierzających do osiągnięcia określonego celu lub misji. Za: *Joint Operations*, 2011, s. XVII.

[85] Warden, 1995: 40—55; Sienkiewicz, Świeboda, 2006: 58; *Strategic War*, 1996; Molander, Riddile, Wilson, 1996. Za: Lakomy, 2013d: 131.

Alexis Bautzmann stwierdził wręcz, iż rozpoczął się proces militaryzacji Internetu, którego przejawem jest powstawanie jednostek wojskowych wyspecjalizowanych w walce w środowisku teleinformatycznym. Sprawiło to jego zdaniem, iż należało ponownie przemyśleć znaczenie takich terminów, jak *bezpieczeństwo* czy *narodowa suwerenność* (Bautzmann, 2012: 80—81). Bruce Berkowitz (1997: 221) pisał natomiast, iż powodem pojawienia się tego typu problemów było przekroczenie „masy krytycznej" przez nowe technologie, które odgrywają fundamentalną rolę zarówno dla wojska, jak i struktur cywilnych. Podobne stanowisko zajęła Myriam Dunn-Cavelty (2012: 103—123), która uznała militaryzację cyberprzestrzeni za jedno ze źródeł globalnych napięć. Można także przytoczyć słowa Bogusława Packa oraz Romualda Hoffmanna, według których „współczesne siły zbrojne zmieniają swój charakter w związku z postępem technologicznym i wejściem w tzw. erę informacyjną. Przewaga, a nawet panowanie w sferze informacyjnej, staje się jednym z najważniejszych obszarów, oddziaływującym bezpośrednio na charakter działań militarnych" (Pacek, Hoffmann, 2013: 71). Symbolicznym wyrazem tych przemian było powstanie amerykańskiego United States Cyber Command (USCYBERCOM) w 2009 roku[86]. Równolegle prace nad stworzeniem odrębnego rodzaju sił zbrojnych działających w sieci rozpoczęło szereg innych państw, w tym np. Wielka Brytania, Rosja oraz Chiny[87].

Wbrew pozorom ze względu na specyfikę cyberprzestrzeni rozwój komponentów wojskowych działających w tym środowisku rodził od samego początku spore wątpliwości. Dotyczyły one nie tylko technicznych możliwości prowadzenia operacji wojskowych w sieci, lecz także ich interpretacji z perspektywy międzynarodowych stosunków politycznych oraz prawa międzynarodowego publicznego. Generał Keith B. Alexander (2007: 58—61) twierdził wręcz, iż przystosowanie wojska do działań w cyberprzestrzeni rodzi podobne problemy jak przystosowanie sił zbrojnych do działań powietrznych w latach 1919—1938. Odpowiedzi na szereg pytań z tym związanych, np. dotyczących skuteczności tradycyjnych zapisów prawa wojny w odniesieniu do cyberprzestrzeni, stały się o tyle istotne, iż zaczęły determinować m.in. prace Organizacji Narodów Zjednoczonych (Bufalini, 2012: 92; Record, 1997: 198—205).

W tym świetle w literaturze specjalistycznej wykształciły się różne sposoby postrzegania tego typu zagadnień. Jedni badacze operacje zbrojne przeprowadzane w cyberprzestrzeni lub za jej pomocą utożsamiali ze zjawiskiem

[86] Warto wspomnieć, iż wielu amerykańskich dowódców uważało, iż celem powołania tego typu struktur jest nie tylko obrona przed cyberatakami, lecz rzeczywista „kontrola cyberprzestrzeni", jak bowiem stwierdził jeden z nich: „jeśli bronisz się w cyberprzestrzeni, to jest już za późno". Za: Clarke, Knake, 2010: 36.

[87] Bautzmann, 2012: 80—81; Giles, 2011; M. Dura: *Cyberdowództwo w Rosji już w 2014 r.* Defence24.pl, 08.10.2013: www.defence24.pl/news_cyberdowodztwo-w-rosji-juz-w-2014-r; dostęp: 13.10.2013.

cyberwojny. W ten sposób do tych zagadnień podchodzili m.in. Samuel Liles, Marcus Rogers oraz Dean Larson (2012: 169—179). Zdaniem innych bardziej zasadny wydaje się termin *walki informacyjnej*. Piotr Sienkiewicz i Halina Świeboda (2009: 84), podkreślając, iż walka taka zawsze była istotnym elementem działań zbrojnych, wyróżnili szereg jej cech: celem jest uzyskanie przewagi informacyjnej nad przeciwnikiem, przeciwnik jest niewidzialny, terenem działań jest cyberprzestrzeń, podstawową formą walki są cyberataki, ich obiektem jest głównie infrastruktura krytyczna, zaś czynnikiem krytycznym pozostaje czas. Jak już sygnalizowano wcześniej, termin *informacyjny* ma stosunkowo szerokie, a często także nie do końca sprecyzowane znaczenie, w niektórych ujęciach może więc budzić wątpliwości natury interpretacyjnej (Liedel, 2011: 53—56). Na tej podstawie *walkę informacyjną* definiuje się bardzo szeroko, np. jako konflikt, w którym „informacja jest jednocześnie zasobem, obiektem ataku i bronią, a zarazem obejmuje on fizyczne niszczenie infrastruktury, wykorzystywanej przez przeciwnika do działań operacyjnych" (Sienkiewicz, Świeboda, 2009: 80; zob. także: Aleksandrowicz, 2014: 44—45). Tak szerokie ujęcie pozwala objąć tym terminem wszystkie rodzaje działań w cyberprzestrzeni, również te, które doprowadziłyby do powstania szkód fizycznych, materialnych. Z jednej strony z perspektywy nauk o obronności tego typu podejście wydaje się w pełni uzasadnione, z drugiej jednak w ujęciu nauk politycznych taka definicja może rodzić pewne wątpliwości, zacierając odmienne cechy poszczególnych cyberzagrożeń oraz wykraczając poza niektóre omówione wcześniej definicje słowa *informacja*. W tym kontekście warto odwołać się do rozważań Freda Schreiera. Jego zdaniem *walka informacyjna* jest pojęciem zdecydowanie szerszym, wykraczającym poza pojęcie *walki w cyberprzestrzeni*, obejmuje ona bowiem nie tylko sieć, ale także działania psychologiczne (PSYOPS), walkę elektroniczną czy wprowadzanie przeciwnika w błąd (*Military Deception*)[88]. Wydaje się więc, iż dla potrzeb niniejszej analizy termin *walki informacyjnej* jest zbyt szeroki. Należałoby go więc zawęzić do kategorii *operacji zbrojnych w cyberprzestrzeni*. Zasadniczym sensem takiego podejścia jest wskazanie, iż domena ta może być wykorzystana do osiągnięcia określonych efektów militarnych, które mogą, lecz wcale nie muszą zawierać się w zjawisku cyberwojny (za: Lakomy, 2013d: 134—135).

W literaturze przedmiotu w kontekście pierwszej wojny, w której wykorzystano cyberprzestrzeń do realizacji „określonego celu lub misji", często wspomina się już o interwencji w Zatoce Perskiej w 1991 roku (Guisnel, 1997a:

[88] Z kolei Martin C. Libicki do walki informacyjnej zaliczył: walkę o przewagę w dowodzeniu i komunikacji, walkę bazującą na przewadze rozpoznania i wywiadu, środki elektromagnetyczne i elektroniczne, działania psychologiczne, wojnę hakerską, ekonomiczną walkę informacyjną oraz właściwą cyberwalkę. Zob. Schreier, 2015, s. 19—21; Libicki, 2007: 16—17; Yagil, 2002: 57—58.

176—180). Jest to jednak stwierdzenie nieco na wyrost. Z jednej strony rzeczywiście była to pierwsza wojna, w której na taką skalę wykorzystano najnowsze technologie teleinformatyczne. W walkach na Bliskim Wschodzie fundamentalną rolę odegrała zdolność do szybkiego zbierania i przetwarzania informacji, co według wielu autorów potwierdziło rewolucję w dziedzinie wojskowości (RMA) (Lekowski, 2011: 265—267). Z drugiej strony podczas wojny doszło do udanych cyberataków na amerykański MILNET, choć należy podkreślić, iż nie miały one żadnego związku z działaniami prowadzonymi przez USA w Zatoce Perskiej[89]. Wydaje się zatem, iż pierwszą wojną, w której cyberprzestrzeń stała się w jakikolwiek sposób areną zmagań przeciwnych stron, był konflikt czeczeński, przeprowadzane przez separatystów ataki komputerowe były jednak wówczas bardzo sporadyczne i stosunkowo niegroźne, nie miały one ponadto charakteru wojskowego, trudno tu więc mówić o operacjach zbrojnych[90]. Po raz kolejny, już na większą skalę, cyberataki towarzyszyły konfliktowi w Kosowie w 1999 roku. Wówczas, jak podają niektóre źródła, ofiarą padły zarówno komputery reżimu w Belgradzie, jak i Kwatery Głównej NATO[91]. Jednak i w tym wypadku trudno mówić o działaniach mających charakter *stricte* militarny. Stany Zjednoczone nie zdecydowały się wówczas na wykorzystanie pełnego potencjału w cyberprzestrzeni w celu wsparcia bombardowań lotniczych. Wynikało to z jednej strony z obaw o prawną interpretację tego typu aktów, z drugiej natomiast Waszyngton nie chciał ujawniać swych rzeczywistych możliwości w tej dziedzinie[92]. W literaturze specjalistycznej wspomina się o amerykańskiej interwencji w Iraku w 2003 roku. Co ciekawe, Biały Dom nie odwołał się wówczas do cyberataków, sieci użyto jednak w walce psychologicznej, wysyłając w przeddzień inwazji wiadomości e-mail do irackich dowódców, nawołujące do poddania się siłom amerykańskim. Jak stwierdzili Richard A. Clarke oraz Robert K. Knake (2010: 12), przyniosło to oczekiwany skutek, gdyż wiele jednostek wojskowych zostało rozpuszczonych do domów jeszcze przed rozpoczęciem inwazji[93].

Wszystkie opisane wyżej wydarzenia, jakkolwiek towarzyszyły działaniom zbrojnym, stanowiły raczej element walki psychologicznej lub propagando-

[89] *The Evolution of U.S. Cyberpower*. AFCEA: www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf; dostęp: 9.09.2013.

[90] Schreier, s. 107; Arquilla, Ronfeldt, 2001: 16—19; Zob. też Carr, 2010: 3; Yagil, 2002: 97.

[91] Cordesman, Cordesman, 2001, s. 34—37; Dunn-Cavelty, 2008: 73—75.

[92] Borger, 1999; S. Myrli: *NATO and Cyber Defence*. NATO Parliamentary Assembly, 173 DSCFC 09 E BIS; J. Carr: *Real Cyber Warfare: Carr's Top Five Picks*. „Forbes" 02.04.2011: www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks; dostęp: 11.09.2013.

[93] *Leaflets and e-mail urge Iraqi commanders to surrender*. „New Straits Times" 21.03.2003, s. 4; C.R. Smith: *Cyber War Against Iraq*. Newsmax.com, 13.03.2003: http://archive.newsmax.com/archives/articles/2003/3/12/134712.shtml, 20.02.2013; dostęp: 11.09.2013.

wej, a więc jedynie pośrednio ułatwiały prowadzenie działań kinetycznych (za: Lakomy, 2013d: 131—132). Sytuacja ta zmieniła się diametralnie w 2007 roku w kontekście izraelskiej operacji *Orchard*, która zakładała zniszczenie syryjskiego ośrodka badań nad bronią jądrową. Ze względu na zaawansowany system obrony przeciwlotniczej reżimu Baszara Al Assada Izrael zdecydował się prawdopodobnie na jego zainfekowanie złośliwym programem, czego efektem było oślepienie syryjskich radarów, które nie wykryły nalotu IDF (ang. *Israel Defense Force*; zob. Rid, 2012). Był to pierwszy i jak dotąd jedyny znany przykład bardzo skutecznego połączenia ataków teleinformatycznych oraz konwencjonalnych działań zbrojnych. Należałoby ponadto wspomnieć o konflikcie zbrojnym na Kaukazie w sierpniu 2008 roku. Doszło wówczas do kampanii teleinformatycznej, której celem były strony internetowe gruzińskiego rządu, najważniejszych przedsiębiorstw, mediów oraz ośrodków naukowych, cyberataki przeciwko rosyjskim witrynom przeprowadzali również sami Gruzini. W tym kontekście warto podkreślić, iż działania w cyberprzestrzeni nie wpłynęły na konwencjonalne działania zbrojne, lecz wpisały się w propagandę wojenną i działania informacyjne prowadzone przez Federację Rosyjską, udało się bowiem częściowo zablokować Tbilisi możliwość prezentowania swojego stanowiska społeczności międzynarodowej wobec wydarzeń, które miały wówczas miejsce na Kaukazie (Lakomy, 2010a: 185; Hollis, 2011).

Na tym tle należałoby więc wskazać na szereg cech tej formy zagrożeń teleinformatycznych. Przede wszystkim warto zauważyć, iż podmiotami zaangażowanymi w tym zakresie pozostają głównie państwa, które mogą wykorzystywać potencjał cyberprzestrzeni do osiągnięcia określonych efektów militarnych, a przez to również politycznych. Działania te charakteryzują się zatem wysokim poziomem zorganizowania i mają bardzo poważne konsekwencje w wymiarze prawnomiędzynarodowym. Z reguły stoją za nimi wyspecjalizowane służby lub siły zbrojne, które posiadają jasno określoną hierarchię i strukturę oraz wyraźnie wyodrębnione cele. Operacje zbrojne w cyberprzestrzeni mogą ponadto przybierać zróżnicowane formy, począwszy od stosunkowo prostych metod, takich jak wykorzystujące sieci *botnet* ataki typu DDoS, a skończywszy na bardziej wysublimowanych technikach, obejmujących np. zastosowanie specjalnych wirusów i robaków komputerowych. Bezpośrednie cele takich akcji mogą być rozmaite, pod warunkiem iż stanowią element realizacji zadania, misji o charakterze militarnym. Mogą np. dotyczyć sparaliżowania określonych usług lub elementów systemów teleinformatycznych, tak jak miało to miejsce w Syrii. Ofiarami tego typu aktów padają z reguły obiekty mające fundamentalne znaczenie dla bezpieczeństwa państwa, w tym elementy infrastruktury krytycznej oraz system obronny. Operacje zbrojne w przestrzeni teleinformatycznej mogą mieć konsekwencje zarówno w wymiarze niematerialnym, jak i materialnym: innymi słowy wiążą się m.in. ze zniszczeniami fizycznymi, utratą lub modyfikacją danych w formie cyfrowej lub osiągnięciem przewagi informacyjnej nad przeciwnikiem

poprzez ograniczenie jego zdolności do pozyskiwania, przetwarzania i przesyłania informacji.

Należy w tym miejscu zaznaczyć, iż operacje zbrojne w cyberprzestrzeni nie są w ujęciu tej pracy tożsame z szerszym zjawiskiem cyberwojny, które zostało omówione w następnym rozdziale. Jak pisał Bolesław Balcerowicz, współcześnie „granice między tym, co jest wojną, a tym, co wojną nie jest, są nieostre i płynne”[94]. W związku z tym w dalszych częściach pracy przyjęto kilka założeń, aby je wyostrzyć. W najprostszym ujęciu różnica między nimi jest taka, jak między operacją zbrojną a konfliktem zbrojnym — nie każda od razu przekształca się w wojnę. Tym samym pojedyncza, odosobniona operacja zbrojna w cyberprzestrzeni, taka jak izraelska misja *Orchard*, nie stanowi elementu konstytutywnego cyberwojny. Jeśli jednak miałaby charakter ciągły, powtarzalny, wówczas taka kwalifikacja jest jak najbardziej zasadna.

Reasumując, należy więc podkreślić, iż głównym założeniem operacji zbrojnych w cyberprzestrzeni jest ułatwienie lub zastąpienie konwencjonalnych działań wojskowych w innych miejscach. Nie muszą być to wbrew pozorom jedynie działania na lądzie i w powietrzu. Jak zauważył Jan Kallberg (2012), współcześnie istnieje nawet możliwość dokonywania cyberataków, które będą miały wpływ na bieg wydarzeń w przestrzeni kosmicznej, doprowadzając do zejścia satelitów z wyznaczonych orbit okołoziemskich. Tego typu aktywność należy więc uznać za jedną z najbardziej zaawansowanych i zarazem najgroźniejszych form zagrożeń bezpieczeństwa teleinformatycznego.

3.4. Cyberwojna

3.4.1. Cyberwojna jako przedmiot debaty naukowej

W świetle postawionego we wstępie celu badawczego charakterystyka zagrożeń teleinformatycznych nie może pominąć jeszcze jednego zagadnienia, jakim jest często podejmowane i kontrowersyjne zjawisko cyberwojny. Wywołuje ono od lat burzliwą debatę naukową i polityczną. Należy zauważyć, iż próżno w niej szukać zgody nie tylko co do wykorzystywanej terminologii w tym zakresie, ale w ogóle charakteru czy wręcz sensu wyodrębnienia tego fenomenu

[94] B. Balcerowicz: *Czym jest współczesna wojna?* Uniwersytet Warszawski: www.pl.ism.uw.edu.pl/index.php?option=com_content&view=article&id=134:prof-dr-hab-bolesaw-balcerowicz-profesor-zwycz&catid=12&Itemid=17; dostęp: 16.09.2013.

(zob. np. Yagil, 2002: 53—57). Podejmując próbę analizy rywalizacji i współpracy państw w cyberprzestrzeni, warto więc szerzej zastanowić się nad tym problemem.

Przede wszystkim należy stwierdzić, iż dyskusja na ten temat rozpoczęła się naturalnie, wraz z coraz szerszym zainteresowaniem rządów przestrzenią teleinformatyczną. Rewolucja technologiczna oraz postępujące procesy komputeryzacji i informatyzacji sprawiły, iż rządy stopniowo zaczęły dostrzegać fakt wielowymiarowych korzyści płynących z wykorzystania technologii ICT. Niektóre z nich, prawidłowo odczytując uwarunkowania omówione w poprzednich rozdziałach, zrozumiały, iż działając w cyberprzestrzeni, mogą realizować określone interesy w środowisku międzynarodowym. Do pierwszych niemilitarnych prób w tym zakresie doszło jeszcze w latach 80. XX wieku. Z jednej strony można by tu wspomnieć o przygotowanym przez państwa Sojuszu Północnoatlantyckiego programie PROMIS, który został wykorzystany do włamywania się do komputerów państw Układu Warszawskiego. Z drugiej strony podobnie działał Związek Radziecki, który w tym okresie wynajął wspomnianego hakera Markusa Hessa, aby wyprowadził wrażliwe dane m.in. z amerykańskiego MIT lub Pentagonu. W obu przypadkach działania te miały jednak charakter eksperymentalny i później na długo zarzucony[95], ponieważ w latach 90. bez względu na dynamicznie rozwijające się zagrożenia teleinformatyczne zdecydowana większość państw zupełnie nie dostrzegała potencjału cyberprzestrzeni. Jedynie kilka państw, w tym USA, Rosja oraz Chiny, szerzej zainteresowało się tą problematyką (zob. Molander, Riddile, Wilson, 1996). Już jednak wówczas m.in. Jean Guisnel (1997a: 257) pisał: „[cyber — M.L.] wojna trwa. Siły wykorzystujące broń ze skomputeryzowanych arsenałów czynią postępy w istniejących sieciach".

Mimo coraz ciekawszych opracowań naukowych rzeczywisty przełom w debacie na ten temat nastąpił dopiero w 2007 roku, kiedy doszło do masowych ataków teleinformatycznych na Estonię. Bez względu na kontrowersje związane z identyfikacją rzeczywistych sprawców należy podkreślić, iż ataki zostały przeprowadzone w wyniku sporu politycznego między Tallinem a Moskwą. Był to pierwszy przypadek w historii, w którym suwerenne państwo zostało na taką skalę zaatakowane przez Internet (Lakomy, 2010b: 61; Lakomy, 2012: 206). W kilka miesięcy później, jak wspomniano, w ramach operacji *Orchard* doszło do połączenia konwencjonalnego ataku wojskowego z akcją w cyberprzestrzeni przeciwko syryjskiemu systemowi obrony przeciwlotniczej. W sierpniu 2008 roku masowe cyberataki wystąpiły podczas konfliktu gruzińsko-rosyjskiego. Podobne wydarzenia miały miejsce również m.in. w Iranie, Kirgistanie, Korei Południowej czy na Litwie. Wszystkie te wydarzenia w zasadniczym stopniu

[95] T. Formicki: *Komandosi cyberprzestrzeni*. „Stosunki Międzynarodowe", 07.11.2007: www.stosunki.pl/?q=node/1106; dostęp: 11.09.2013; Lakomy, 2010b: 57.

zintensyfikowały rozważania poświęcone rywalizacji i walce państw w sieci, zdano sobie bowiem sprawę, iż ze względu na jej unikalne właściwości staje się ona coraz bardziej dogodnym obszarem realizowania określonych interesów w środowisku międzynarodowym.

Jak słusznie zauważyli Krzysztof Liedel i Paulina Piasecka (2011: 17), próba zdefiniowania „wojny cybernetycznej" jest poważnym wyzwaniem, gdyż nie został ustalony powszechnie akceptowany aparat pojęciowy w obszarze walki informacyjnej, a poszczególne koncepcje adekwatne są do koncepcji i podejść określonych „szkół myślenia". Rzeczywiście, w wieloletniej debacie naukowej poświęconej temu zagadnieniu wykorzystuje się bardzo zróżnicowane pojęcia[96]. W literaturze przedmiotu oraz w dokumentach państwowych stosuje się m.in. takie terminy, jak *cyberwojna*, *cyberwalka* (*cyberwarfare*), *wojna informacyjna* (*wojna ery informacyjnej*) czy *wojna cybernetyczna*[97]. Pojawia się także często pojęcie *netwar*, która zdaniem Johna Arquilli oraz Davida Ronfeldta oznacza konflikt teleinformatyczny o niższej od cyberwojny intensywności, toczony na poziomie społeczeństw (a więc np. haktywistów, terrorystów, przestępców), a nie struktur państwowych[98]. Ponadto, jak wspomniano, część badaczy nie widzi różnicy między pojedynczą operacją zbrojną w sieci a cyberwojną. Sytuację tę dodatkowo komplikuje fakt, iż zdaniem pewnej grupy naukowców dotychczasowe wydarzenia i przykłady ścierania się interesów państw w cyberprzestrzeni nie stanowią bynajmniej podstaw do wyodrębnienia takiego zjawiska. Wśród sceptyków, którzy odrzucają terminy *cyberwojny* bądź *wojny informacyjnej*, szczególnie często przytacza się opinię Thomasa Rida (2012), autora głośnego opracowania *Cyber War Will Not Take Place*, według którego dotychczasowe incydenty teleinformatyczne nie stanowią wystarczającego dowodu na zaistnienie tego zjawiska, gdyż nie spełniają trzech kryteriów właściwych wojnie: śmiercionośności, instrumentalności oraz politycznej motywacji. Podobne stanowisko zajął Eugene Spafford, który również zauważył, iż najpoważniejsze incydenty teleinformatyczne nie dają podstaw do wyodrębnienia pojęcia *cyberwojny* (*Virtual Criminology Report*, 2009: 8—12). Odmienne i bardzo ciekawe podejście zaprezentowali z kolei Piotr Sienkiewicz i Halina Świeboda (2009: 80), którzy zauważyli, iż „obecnie słusznie uważa się, że *cyberwar*, *infowar*, walka informacyjna, cyberterroryzm, *netwar*, informacyjni wojownicy, informacyjna

[96] Warto przypomnieć, iż termin *wojny informacyjnej* wykorzystał po raz pierwszy Thomas Rona z Boeing Corporation już w 1976 roku, natomiast w 1993 roku w artykule Naval Postgraduate School pojawiło się pojęcie „cyberwojny". Zob. Geers, 2011: 25.

[97] Przy czym np. Martin C. Libicki krytykował kategorię *wojny informacyjnej* jako pojęcie zbyt szerokie. Zob. np. Bronk, 2011: 5; Sienkiewicz, 2003; Sienkiewicz, Świeboda, 2009; Libicki, 2001; Carr, 2010; Blane, ed., 2001; Shimeall, 2001.

[98] W innym miejscu autorzy zdefiniowali to pojęcie następująco: „wykorzystanie sieciowych form organizacji, doktryn, strategii i technologii dobranych do ery informacyjnej". Za: Arquilla, Ronfeldt, 2001: IX, 7.

dominacja, obrona w cyberprzestrzeni (*cyberspace defense*) czy informacyjny chaos to tylko neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia *wojny ery informacyjnej* (*information age war*)".

Wątpliwości formułowane przez Thomasa Rida czy Eugene'a Spaffordа wydają się jednak nie do końca przemyślane. Przede wszystkim zbyt mocno utożsamiają oni cyberwojnę z konwencjonalnym konfliktem zbrojnym, który rzeczywiście charakteryzuje się śmiercionośnością. Mając na uwadze specyfikę działań w cyberprzestrzeni, należy zauważyć, że zdecydowana większość cyberataków wiąże się ze szkodami niematerialnymi. Nie oznacza to jednak, iż nie istnieje możliwość powstania zniszczeń fizycznych, które mogłyby doprowadzić do śmierci dotkniętych nimi jednostek. Najbardziej doniosłym przykładem tego typu incydentu było wykorzystanie robaka *Stuxnet*, który doprowadził do awarii wirówek wzbogacających uran w Iranie. Należy również wspomnieć o przeprowadzonym przez Stany Zjednoczone w 2007 roku doświadczeniu o kryptonimie *Aurora*. W wyniku cyberataku amerykańskim specjalistom udało się dokonać sabotażu generatora prądotwórczego w elektrowni, przez co udowodnili, iż manipulacja danymi w formie cyfrowej może doprowadzić do bardzo poważnych w skutkach zniszczeń materialnych[99]. W tym kontekście łatwo można wyobrazić sobie sytuację, w której awaria określonych urządzeń elektronicznych kontrolujących funkcjonowanie np. infrastruktury krytycznej (sieci elektroenergetycznej, systemu ochrony zdrowia czy dystrybucji żywności) mogłaby w konsekwencji doprowadzić do śmierci ludności cywilnej. Tym samym cyberataki przeprowadzane przez państwa mogą, ale wcale nie muszą wiązać się ze stratami ludzkimi.

Nie można się również zgodzić z wnioskami Thomasa Rida dotyczącymi braku instrumentalności oraz politycznej motywacji przeprowadzanych przez państwa cyberataków. Jak wskazano w poprzednich rozdziałach, istnieje wiele czynników, które sprawiają, iż cyberprzestrzeń jest coraz bardziej dogodną domeną realizowania interesów i celów polityki zagranicznej przez państwa. Można do nich zaliczyć takie kwestie, jak „ageograficzność" przestrzeni teleinformatycznej, niższe koszty działania, mniejsze ryzyko wykrycia lub poniesienia konsekwencji ataku, faworyzowanie działań ofensywnych nad defensywnymi, wysoki potencjał z perspektywy działań propagandowych i informacyjnych, brak skutecznych i zaktualizowanych regulacji prawa międzynarodowego, łatwa do osiągnięcia anonimowość, brak systemów wczesnego ostrzegania i utrudnione działania wywiadowcze, brak odpowiednika systemu MAD (zob. np. Schreier, 2015).

Na tym tle należy stwierdzić, iż poszczególne kraje od lat odwołują się do rozmaitych działań w cyberprzestrzeni w celu osiągnięcia określonego efektu,

[99] Lewis, 2012; J. Meserve: *Sources: Staged cyber attack reveals vulnerability in power grid*. CNN, 26.09.2007: http://edition.cnn.com/2007/US/09/26/power.at.risk; dostęp: 13.09.2013.

głównie w wymiarze politycznym, ale czasami także gospodarczym bądź militarnym (szerzej na ten temat w kolejnych rozdziałach). Wydaje się, iż jest to główny czynnik, który wskazuje na potrzebę wyodrębnienia nowego terminu charakteryzującego właśnie ścieranie się interesów rządów przy wykorzystaniu potencjału cyberprzestrzeni. Powstaje więc pytanie: czy zasadne jest stosowanie terminu *wojny ery informacyjnej* czy innego popularnego pojęcia, jakim jest np. *cyberwojna*? Jak wskazano wcześniej, terminy oparte na kategorii informacji, jakkolwiek w pełni zasadne z pewnego punktu widzenia, niekoniecznie muszą być przydatne do prowadzonej analizy działań państw w przestrzeni teleinformatycznej w ujęciu politologicznym. Wojna ery informacyjnej jest bowiem pojęciem zdecydowanie szerszym, obejmującym również działania niezwiązane bezpośrednio z cyberprzestrzenią, co oznacza, iż można to pojęcie zawęzić, odwołując się do terminu *cyberwojny*.

Jak wskazano wyżej, głównym powodem wyodrębnienia się tego pojęcia była świadomość, iż państwa w procesach ścierania się interesów na arenie międzynarodowej coraz częściej odwołują się do cyberataków. Brakuje jednak konsensusu wśród specjalistów, jeśli chodzi o jednoznaczne rozumienie tego terminu. Część z nich *cyberwojnę*, *wojnę sieciową* lub *cybernetyczną*, utożsamia jedynie z wykorzystaniem przestrzeni teleinformatycznej jako piątego teatru wojny. Oznacza to, iż byłaby ona tym samym co omówione już *operacje zbrojne w cyberprzestrzeni*. Według innych jest to jednak zjawisko zdecydowanie szersze, wykraczające poza *stricte* wojskowe zastosowanie sieci. Warto więc przedstawić najciekawsze definicje, które pojawiły się w literaturze specjalistycznej.

W tym kontekście można rozpocząć od popularnej definicji USlegal.com, według której *cyberwojna* dotyczy „masowego, skoordynowanego, cyfrowego ataku na rząd [dokonany — M.L.] przez inny [rząd — M.L.] lub przez dużą grupę obywateli. Jest to działanie państwa zmierzające do penetracji komputerów lub sieci innego narodu w celu dokonania zniszczeń lub zakłóceń”[100]. James A. Lewis (2012: 2) z Center for Strategic and International Studies stwierdził, iż

> wykorzystanie technologii sieciowych oraz eksploatacja cyberprzestrzeni do działań wywiadowczych i ataku stały się normalnym aspektem działań wojskowych. Cyberwalka będzie obejmowała zakłócanie istotnych usług sieciowych oraz danych, uszkodzenia infrastruktury krytycznej oraz stwarzanie stanu niepewności i wątpliwości wśród dowódców i liderów politycznych przeciwnika.

Wspomniani już Krzysztof Liedel i Paulina Piasecka (2011: 17—18) uznali *cyberkonflikt* za

[100] *Cyber Warfare*. USLegal.com: http://definitions.uslegal.com/c/cyber-warfare; dostęp: 13.09.2013.

> konflikt angażujący różnorodne systemy ludzi, rzeczy, procesów i postrzegania, które związane są z sieciami komputerowymi, choć niekoniecznie całkowicie skomputeryzowane. Konfliktem cybernetycznym będzie zatem każdy konflikt, w którym sukces lub porażka są dla większości jego uczestników uzależnione od działań prowadzonych w sieciach komputerowych. W związku z tym tak długo, jak długo Internet pozostanie na tyle otwarty, jak jest dzisiaj, konflikty prowadzone na jakiejkolwiek płaszczyźnie będą podlegały „cybernetyzacji".

Wyróżnili oni trzy rodzaje cyberkonfliktów: aktywizm obejmujący działalność wspierającą, niedestrukcyjną, haktywizm będący kombinacją aktywizmu i działań przestępczych oraz cyberterroryzm stanowiący „politycznie motywowany atak lub groźbę ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach realizacji daleko idących politycznych i społecznych działań" (Ibidem). Ciekawe ujęcie zaproponowali również eksperci brytyjskiego ośrodka badawczego Chatham House, według których *cyberwojna* może być

> konfliktem pomiędzy państwami, ale również w różnym stopniu może angażować aktorów niepaństwowych. W konflikcie rozgrywającym się w cyberprzestrzeni niezwykle trudno jest sprecyzować zakres i zasięg ataku; cel może mieć charakter militarny, przemysłowy lub cywilny lub może nim być przestrzeń na serwerze wykorzystywana przez różnych klientów, z których tylko jeden może być obiektem intencjonalnego ataku[101].

Ponadto ich zdaniem „wojna w cyberprzestrzeni umożliwia aktorom osiąganie zamierzonych celów politycznych i strategicznych bez konieczności angażowania się w konflikt zbrojny" (Ibidem). Z kolei Charles Billo oraz Welton Chang (2004: 7) uznali, iż zjawisko to obejmuje „jednostki zorganizowane wokół granic państwowych, dokonujące ofensywnych i defensywnych operacji, wykorzystując komputery do ataku na inne komputery lub sieci za pomocą środków elektronicznych". Ich zdaniem fenomen ten ma w zasadniczym stopniu wpływać na charakter przyszłych konfliktów zbrojnych. Julie E. Mehan (2008: 28) wyróżniła 4 klasy cyberwojen:

- klasę I obejmującą ochronę osobistych danych w sieci,
- klasę II obejmującą przemysłowe i gospodarcze szpiegostwo wymierzone w narody, korporacje i uniwersytety,
- klasę III — globalną wojnę i terroryzm, w tym również cyberterroryzm oraz ataki przeciwko elementom infrastruktury krytycznej,
- klasę IV charakteryzującą się wykorzystaniem technik z klas I—III równocześnie z realizacją operacji wojskowych w celu uzyskania przewagi na polu walki.

[101] P. Cornish, ed., 2010, s. 2 (cyt. za: Bania, 2012: 188—189).

Klaus-Peter Saalbach (2012: 4—5) stwierdził, iż *cyberwojna* „jest kombinacją terminów *wojny* oraz *cyberprzestrzeni* i oznacza konflikt wojskowy wykorzystujący środki technologii informacyjnych. W praktyce jest to atak na komputery oraz ich dane, sieci komputerowe oraz systemy zależne od komputerów". Co ciekawe, autor zauważył, iż cyberwojna jest zjawiskiem jakościowo odmiennym od cyberterroryzmu czy cyberszpiegostwa. Nils Melzer (2011: 4) przyjął zdecydowanie bardziej uproszczone podejście twierdząc, iż jest to „walka w cyberprzestrzeni za pomocą cyberśrodków i metod". Podobne stanowisko zajęli Andrew Colarik i Lech Janczewski (2012: 31—33), według których jest to po prostu konflikt, wojna w cyberprzestrzeni. Richard A. Clarke oraz Robert K. Knake uznali natomiast, że jest to „działalność państw, mająca na celu penetrację systemów i sieci komputerowych innych podmiotów międzynarodowych dla dokonania określonych zniszczeń lub zakłóceń" (Clarke, Knake, 2010: 6; Lakomy, 2011a: 151—152). Na tym tle warto również przytoczyć ciekawą propozycję przygotowaną wspólnie przez naukowców rosyjskich i amerykańskich z Moskiewskiego Uniwersytetu Państwowego oraz EastWest Institute. Rozróżnili oni w dokumencie z kwietnia 2011 roku terminy *cyberkonfliktu* oraz *cyberwojny*. Przez *cyberkonflikt* rozumieli oni „napiętą sytuację pomiędzy państwami lub grupami zorganizowanymi, w której niemile widziane cyberataki spotykają się z odwetem" (*Critical Terminology Foundations*, 2011: 29—30). Za *cyberwojnę* uznali natomiast cyberkonflikt między państwami, który uległ eskalacji. W jej ramach aktorzy państwowi dokonują cyberataków przeciwko „cyberinfrastrukturze", które stanowią część szerszej kampanii militarnej (Ibidem, s. 29—30). Warto również przytoczyć definicję sformułowaną przez ekspertów University of Peace, którzy w zaproponowanym przez siebie modelu rezolucji Rady Bezpieczeństwa ONZ stwierdzili, iż jest to

> wykorzystanie komputerów lub elektronicznych środków przez rząd za jego wyraźną wiedzą bądź akceptacją przeciwko innemu państwu lub własności prywatnej […] obejmujące: intencjonalny dostęp, przechwytywanie danych lub zniszczenie cyfrowej lub cyfrowo sterowanej infrastruktury; produkcję oraz dystrybucję urządzeń, które mogą być wykorzystane do zakłócenia działań krajowych" (*Resolution 1113, 2011*).

Definicja Departamentu Obrony Stanów Zjednoczonych wykorzystuje natomiast termin *cyberoperacji*. Rozumie się przez to „wykorzystanie cyberzdolności, których głównym motywem jest uzyskanie określonych celów lub efektów wojskowych lub poprzez cyberprzestrzeń". Congressional Research Service uznało *cyberwojnę* za „różne aspekty obrony i ataku sieci informacyjnych i komputerowych w cyberprzestrzeni, jak również zablokowanie przeciwnikowi możliwości tego typu działalności" (*Department of Defense Dictionary*, 2013; Schreier, 2015: 17).

Na podstawie przytoczonych wyżej definicji widać więc wyraźnie, iż w literaturze specjalistycznej oraz w dokumentach państwowych funkcjonuje bardzo szerokie spektrum sposobów wyjaśniania tego zjawiska. Część z nich skupia się wyłącznie na jej aspektach technicznych, inne z kolei sprowadzają to zagadnienie do zagadnień *stricte* militarnych. Niektóre z propozycji naukowych cyberwojnę traktują jednak nieco szerzej, dostrzegając fakt, iż może ona obejmować zróżnicowane formy rywalizacji państw w cyberprzestrzeni.

3.4.2. Definicja cyberwojny

W oparciu o te rozważania warto zatem podjąć próbę sformułowania kompleksowej definicji tego pojęcia, która byłaby przydatna do analizy prowadzonej w dalszej części pracy. Aby tego dokonać, należałoby jednak wyjść od zagadnienia z reguły pomijanego przez innych autorów, czyli zjawiska samej wojny. Jest to o tyle problematyczne, iż od wieków trwają dyskusje poświęcone temu, czym w zasadzie ona jest. Już w czasach starożytnych Arystoteles określał wojnę nie jako cel sam w sobie, lecz środek prowadzący do pokoju[102]. Analizując to pojęcie, częstokroć przywołuje się klasyczną pracę *O wojnie* Carla von Clausewitza. W wielu wypadkach jego myśl upraszcza się i skraca, twierdząc, iż wojna jest swoistym „przedłużeniem polityki". W rzeczywistości stanowisko tego wybitnego teoretyka wojskowości było zdecydowanie bardziej złożone. Przede wszystkim von Clausewitz (2010: 15—31) podkreślał, iż wojna jest „aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli". Wskazał on wiele istotnych elementów składających się na to zjawisko. Wśród zauważonych przez niego prawidłowości należy wymienić następujące stwierdzenia:

1. Użycie siły następuje „aż do ostateczności".
2. Celem jest obezwładnienie wroga.
3. Wojna nie jest nigdy aktem odosobnionym, nie składa się z jednego, krótkotrwałego uderzenia.
4. Wynik wojny nie jest nigdy bezwzględny.
5. Cel polityczny jest pierwotnym motywem wojny.
6. Wojna jest czynem politycznym.
7. „Wojna jest nie tylko czynem politycznym, lecz i prawdziwym narzędziem polityki, dalszym ciągiem stosunków politycznych, przeprowadzeniem ich innymi środkami".
8. Każdą wojnę można uważać za działanie polityczne.

[102] *Aristotle*. Quotationspage: www.quotationspage.com/quotes/Aristotle/31; dostęp: 16.09.2013.

Od XIX wieku w literaturze naukowej nastąpiła daleko idąca ewolucja, jeśli chodzi o podejście do tego zjawiska. Bazując na tych klasycznych i fundamentalnych konstatacjach, w XX wieku dostrzeżono nowe, wcześniej niezauważone lub niespotykane cechy konfliktów zbrojnych. Już w 1912 roku Georges Sorel pisał, iż wojna jest aktem politycznym, za pomocą którego państwa, które nie są w stanie dojść do porozumienia w sporze dotyczącym ich obowiązków, praw oraz interesów, odwołują się do sił zbrojnych w celu sprawdzenia, kto jest silniejszy i może narzuć swą wolę pokonanemu. Nieco później Alvin Johnson uznał ją za „konflikt zbrojny pomiędzy grupami populacji wyobrażonymi jako rasy, plemiona, państwa lub mniejsze geograficzne jednostki, partie polityczne lub religijne, klasy ekonomiczne". Karl Deutsch i Dieter Senghaas scharakteryzowali to zjawisko jako zorganizowaną przemoc na dużą skalę, przygotowaną i podtrzymywaną za pomocą przemocy i legitymizacji pochodzących od państwa i wymierzoną przeciwko innemu państwu lub *quasi*-państwu. Quincy Wright z kolei uważał wojnę za „stan prawny […] pozwalający rozwiązywać konflikt przez użycie siły zbrojnej". Szczególnie w ujęciu prawnym bardzo często utożsamiało się wojnę ze „stanem walki orężnej między państwami"[103].

Powyższe definicje, formułowane jeszcze przed okresem pozimnowojennym, mają szereg słabych stron. Przemiany w środowisku międzynarodowym po 1989 roku sprawiły, iż tradycyjne ujęcia konfliktów zbrojnych uległy częściowej dezaktualizacji, na co wskazywał Bolesław Balcerowicz. Przede wszystkim akcentuje się, iż wojna niekoniecznie musi wynikać z pobudek politycznych, jej motywem może być bowiem np. interes gospodarczy lub religijny. Po drugie powstaje pytanie: czy obecność państwa i wojska są elementami niezbędnymi, aby dany konflikt zbrojny uznać za wojnę? Po trzecie: reinterpretacji w świetle wydarzeń ostatnich lat wymaga również pojęcie *zorganizowanej przemocy zbrojnej*[104]. Wszystkie wymienione wyżej wątpliwości wynikają z faktu, iż charakter wojen zmienia się wraz z kolejnymi okresami historycznymi oraz postępem naukowo-technicznym. Wojny znane w XIX i XX wieku, mające charakter masowy, po 1989 roku w dużej mierze przestały występować, pojawiła się bowiem szeroka gama konfliktów, które zgodnie z przytoczonymi wyżej definicjami nie powinny być nazywane wojnami[105].

W tym świetle Przemysław Żurawski vel Grajewski zaproponował ciekawe podejście, zgodnie z którym konflikt, aby mógł być uznany za wojnę, powinien charakteryzować się trzema cechami. Po pierwsze muszą ze sobą walczyć co najmniej dwie strony, z których przynajmniej jedna musi stanowić reprezentację militarną rządu znajdującego się u władzy. Gdy żadna ze stron nie reprezentuje

[103] Za: Bierzanek, Symonides, 2002: 379; B. Balcerowicz: *Czym jest współczesna wojna?…*, op.cit.; van der Dennen, 1980.

[104] B. Balcerowicz: *Czym jest współczesna wojna?…*, op.cit.

[105] Szerzej: Regina-Zacharski, 2010/2011.

legalnego rządu, wówczas uznaje się konflikt za niepaństwowy. Po drugie każda ze stron powinna posiadać centrum planowania i dowodzenia. Po trzecie działania wojenne powinny mieć charakter ciągły, nie powinny stanowić serii spontanicznych akcji. Na tej podstawie ustanowiono wiele definicji wojny. Bywa ona współcześnie ujmowana np. jako „zorganizowana, zbiorowa konfrontacja oparta na przemocy" (za: Żurawski vel Grajewski, 2012: 43).

Mając na uwadze powyższe rozważania, należy stwierdzić, iż nie ma jednej, powszechnie przyjętej definicji wojny, jest to jednak zjawisko, które ma pewne cechy charakterystyczne, nie tylko elementy wyodrębnione przez Przemysława Żurawskiego vel Grajewskiego. Przede wszystkim wojna jako taka jest czynem politycznym, choć może wynikać z różnorodnych motywacji, zarówno politycznych, gospodarczych, jak i kulturowych. Jest to zatem zjawisko, które posiada doniosłe reperkusje prawne i polityczne. Należy ponadto stwierdzić, iż cechą szczególną wojny jest użycie przemocy, przez co można rozumieć zastosowanie wobec przeciwnika określonego uzbrojenia[106].

W tym świetle zjawisko cyberwojny ma charakter szczególny. Jak stwierdzono wyżej, konflikty zbrojne w każdej epoce historycznej miały swoje wyjątkowe cechy. Stało się to szczególnie widoczne właśnie na początku XXI wieku w świetle działań prowadzonych w cyberprzestrzeni. Ponownie można tu odwołać się do Carla von Clausewitza (2010: 15), który wyjaśniał tę tendencję, pisząc, iż przemoc „uzbraja się w wynalazki sztuki i nauki, aby stawić czoło przemocy". Zgodnie z tymi słowami wraz z opisaną już rewolucją informatyczną i rewolucją w sprawach wojskowych (RMA) dostrzeżono możliwość wykorzystania cyberprzestrzeni do operacji militarnych. Masowe przedsięwzięcia w tym wymiarze stały się więc pełnoprawną częścią konfliktów, jeśli przyjmiemy, iż przez przemoc rozumie się również zastosowanie broni cybernetycznej (np. robaków komputerowych).

Aktywność wojskowa w cyberprzestrzeni nie jest jednak jedynym aspektem szkodliwej działalności państw online. Oprócz niej występują także działania, które mogą zostać scharakteryzowane jako cyberterroryzm lub cyberszpiegostwo. W obu przypadkach agencje rządowe angażują się w przedsięwzięcia, które posiadają znaczną część omówionych wcześniej cech wojny. Problem w przypadku cyberterroryzmu polega na tym, iż nie są to z reguły operacje ciągłe, lecz ograniczone czasowo. Co prawda mamy tu do czynienia z motywowaną politycznie przemocą oraz bardzo poważnymi reperkusjami dla bezpieczeństwa, mają one jednak charakter raczej odosobniony. Jeśli chodzi zaś o cyberszpiegostwo, analiza tego typu ataków komputerowych w ostatnich latach pozwala sądzić, iż mają one często charakter ciągły i zorganizowany, lecz nie wiążą się bezpośrednio z namacalnymi szkodami. Przyjmując takie założenia, należałoby stwierdzić, iż cyberwojna, bazując jedynie na scharakteryzowanych już cechach

[106] B. Balcerowicz: *Czym jest współczesna wojna?…*, op.cit.

tradycyjnego konfliktu zbrojnego, powinna obejmować wyłącznie prowadzone przez dłuższy czas operacje wojskowe w cyberprzestrzeni.

Takie podejście, jakkolwiek z pewnej perspektywy jak najbardziej słuszne, nie pozwoliłoby jednak szerzej ująć całego spektrum rywalizacji i starć państw w cyberprzestrzeni. Z punktu widzenia stosunków międzynarodowych *cyberwojnę* można by rozumieć nieco szerzej: jako zjawisko obejmujące nie tylko walkę zbrojną w przestrzeni teleinformatycznej, lecz również wszelkie przejawy dokonywanych przez państwa poważnych aktów cyberterroryzmu i cyberszpiegostwa. Zaliczenie ataku cyberterrorystycznego do elementów składowych cyberwojny wymagałoby jednak spełnienia przez niego kilku warunków. Przede wszystkim musiałby on być przeprowadzony przez państwo/państwa i wymierzony w inny podmiot stosunków międzynarodowych. Po drugie celem powinny być obiekty o żywotnym znaczeniu z perspektywy bezpieczeństwa narodowego (infrastruktura krytyczna, system obronny). Po trzecie działania cyberterrorystyczne powinny mieć charakter masowy i powtarzalny, trudno byłoby zatem pojedynczy, choć poważny atak komputerowy uznać za cyberwojnę w sytuacji, w której miałby on niewielką skalę i czas trwania.

Większe wątpliwości powstają w kontekście zaliczenia do cyberwojny aktów cyberszpiegowskich. Jest to tym wyraźniejsze, iż konwencjonalna działalność wywiadowcza z reguły tego typu dylematów nigdy nie wywoływała. Jest to zagadnienie niezwykle trudne do jednoznacznej oceny, ponieważ cyberszpiegostwo z zasady nie wiąże się z przemocą. Problem ten bywa często podnoszony w Stanach Zjednoczonych, które są bezspornie najczęstszym celem cyberataków o charakterze wywiadowczym, szczególnie pochodzenia chińskiego. Skala tych incydentów jest ogromna, co sprawia, iż problem ten jest poruszany przez najwyższe czynniki państwowe[107]. Z jednej strony włamania takie nie prowadzą z reguły do wyraźnych szkód dla infrastruktury krytycznej, systemu obronnego bądź innych urządzeń i systemów powiązanych z cyberprzestrzenią, z drugiej jednak strony utrata wrażliwych danych w formie cyfrowej stanowi bardzo poważne zagrożenie bezpieczeństwa, tym bardziej, jeśli skala incydentów jest bardzo wysoka. Mając na uwadze coraz wyraźniejszą praktykę niektórych państw, polegającą na wykorzystaniu cyberprzestrzeni do nielegalnego zbierania informacji, wydaje się zatem zasadne zaliczenie również działań cyberszpiegowskich do zjawiska cyberwojny.

Reasumując, zaprezentowane wyżej rozważania stanowią podstawę do stworzenia definicji zjawiska *cyberwojny*. Rozwijając propozycję Richarda A. Clarke'a oraz Roberta K. Knake'a, można ją określić jako „powtarzalną działalność państw i ich organizacji mającą na celu penetrację systemów i sieci tele-

[107] *Exposing One of China's*, 2012; *Cyber Espionage*, 2011, s. 7; *Exclusive: Arrested spy compromised China's U.S. espionage network: sources*. Reuters: www.reuters.com/article/2012/06/15/us-china-usa-espionage-idUSBRE85E06G20120615; dostęp: 22.09.2013.

informatycznych innych podmiotów międzynarodowych w celu dokonania określonych zniszczeń, zakłóceń lub pozyskania informacji o żywotnym znaczeniu dla ich bezpieczeństwa". W takim ujęciu posiada ona kilka cech charakterystycznych. Przede wszystkim nie można jej bezwzględnie utożsamiać z tradycyjnym rozumieniem wojny, nie odbiega ona jednak zasadniczo od ujęć nowoczesnych, dostrzegających wielowymiarowość i asymetryczność konfliktów zbrojnych. W literaturze specjalistycznej zgodnie z kryterium sposobu prowadzenia wojny wyróżnia się konflikty pierwszej, drugiej, trzeciej, czwartej generacji oraz wojny hybrydowe. Wojny czwartej generacji to konflikty asymetryczne, które cechują się długotrwałością, wykorzystaniem technik terrorystycznych, decentralizacją, transnarodowością czy zanikiem podziału na front i tyły. Z kolei za wojny hybrydowe uznaje się

> nowoczesne wojny toczone z wykorzystaniem przez strony wojujące wszelkich dostępnych taktyk walki, zarówno regularnych, nieregularnych, jak i cybernetycznych, z możliwością zastosowania broni masowego rażenia oraz z towarzyszeniem wojny informacyjnej, psychologicznej i propagandowej. […] Granica między działaniami partyzanckimi a terrorystycznymi jest w tego typu konfliktach płynna[108].

Na tej podstawie należy stwierdzić, iż cyberwojna wpisuje się w kategorię wojen hybrydowych. Zgodnie z przyjętą definicją oraz praktyką ostatnich lat, można przyjąć, iż spełnia ona większość cech nowoczesnych wojen:

1. Dotyczy co najmniej dwóch państw[109].
2. Każda ze stron ma centrum planowania i dowodzenia.
3. Ma charakter ciągły, masowy.
4. Ma różnorodne motywacje, choć jest aktem politycznym.
5. Odwołuje się do specyficznie rozumianej przemocy, wykorzystując ataki komputerowe jako środki walki.

Takie ujęcie cyberwojny akcentuje, iż współcześnie dzięki cyberprzestrzeni państwa mogą atakować siebie nawzajem, nie ryzykując skutków podobnych do tego, co miałoby to miejsce w przypadku tradycyjnego konfliktu zbrojnego. Wynika to z faktu, iż przestrzeń teleinformatyczna jest środowiskiem unikalnym, w którym nie obowiązuje większość prawideł znanych z wojen XX wieku. W tym kontekście można przywołać rozważania Krzysztofa Liedela i Pauliny

[108] W tym kontekście wspomina się również o wojnach sieciocentrycznych. Zob. Żurawski vel Grajewski, 2012: 61—62; Piasecka, 2014.

[109] Bazując na definicji Przemysława Żurawskiego vel Grajewskiego, należy pamiętać, iż mogą występować sytuacje, w których długotrwałe starcie w cyberprzestrzeni ma miejsce między państwem a podmiotem pozapaństwowym. Tego typu zjawisko nie zawiera się jednak w pojęciu *cyberwojny*, lecz bliżej mu do wspomnianej już kategorii *netwar*. Zob. Arquilla, Ronfeldt, 2001: IX, 7.

Piaseckiej (2011: 27), których zdaniem „cyberwojna zmienia rozumienie tego, co stanowi atak — w przeciwieństwie do wcześniejszych wojen i konfliktów cyberwojna nie musi oznaczać fizycznego zniszczenia przeciwnika, a jedynie uderzenie w krytyczne elementy jego systemu informacyjnego i komunikacyjnego". Tak rozumiana może, lecz nie musi towarzyszyć konwencjonalnemu starciu dwóch państw. Jako taka może być zjawiskiem właściwym wyłącznie dla cyberprzestrzeni, podczas gdy siły zbrojne na lądzie, wodzie i w powietrzu pozostaną bezczynne. Upowszechnieniu tej formy rywalizacji państw sprzyja fakt, iż nie wypracowano dotychczas skutecznych i powszechnie obowiązujących regulacji prawno-politycznych w tej dziedzinie. Ponadto obecnie to przede wszystkim rządy (oraz niektóre korporacje) dysponują wystarczającym potencjałem (środkami finansowymi, zapleczem technicznym i *know-how*), aby dokonywać poważnych, zorganizowanych cyberataków wymierzonych w obiekty o żywotnym znaczeniu dla bezpieczeństwa innych państw. Potwierdza to opracowanie szeregu zaawansowanych złośliwych programów, takich jak *Stuxnet* czy *Duqu*[110]. Zjawisko cyberwojny stanowi dowód na to, iż ataki teleinformatyczne stały się nowym instrumentem realizowania interesów przez państwa i ich organizacje w środowisku międzynarodowym (zob. Myrli, 09 E BIS; Healey, van Bochoven, 2012).

[110] S. Bagchi: *„Countries like India are already realizing the potential of cyber security"*. CXO Today, 05.02.2013: www.cxotoday.com/story/countries-like-india-have-already-realized-the-potential-of-cyber-security; dostęp: 25.02.2013; *Gauss: Nation-state cyber-surveillance meets banking Trojan*. Securelist, 09.08.2012: www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan; dostęp: 25.02.2013.

Rozdział 4

Cyberprzestrzeń jako nowy wymiar rywalizacji państw

Rozważania z poprzednich rozdziałów pozwalają zaryzykować stwierdzenie, iż działania w cyberprzestrzeni stają się stopniowo coraz istotniejsze dla całokształtu stosunków międzynarodowych. Omówione powyżej zagrożenia teleinformatyczne jasno wskazują na fakt, iż współcześnie ich źródłem są różnorodnie motywowane podmioty, zarówno o charakterze państwowym, jak i pozapaństwowym. Dzięki swym wyjątkowym cechom cyberprzestrzeń staje się obecnie coraz dogodniejszą domeną realizowania partykularnych interesów w wymiarze lokalnym, regionalnym, jak i globalnym. Zwrócili na to uwagę m.in. autorzy *Białej księgi bezpieczeństwa narodowego RP* (2013: 12), którzy jednoznacznie stwierdzili, iż „aktywność terrorystów przenosi się również do cyberprzestrzeni, która w coraz większym stopniu będzie się stawać obszarem rywalizacji i konfrontacji, także między państwami".

Mając to na uwadze, warto podjąć próbę weryfikacji tej hipotezy w oparciu o szereg studiów przypadków. Dokładne zbadanie czynników determinujących tego typu zaangażowanie, przebiegu cyberataków oraz ocena ich reperkusji z punktu widzenia celów i środków polityki zagranicznej pozwoli stwierdzić, czy tego typu tendencje rzeczywiście występują w środowisku międzynarodowym od początku XXI wieku.

4.1. „Pierwsza cyberwojna" w Estonii

Analizę przypadków rywalizacji państw w cyberprzestrzeni warto rozpocząć od studium „pierwszej cyberwojny", która miała miejsce w kwietniu i maju 2007 roku między Estonią a Rosją[1]. Aby zrozumieć charakter i powody tych wydarzeń, należałoby na wstępie omówić uwarunkowania stosunków bilateralnych obu państw. Mają one długą i skomplikowaną przeszłość, której źródłem była litewsko-polsko-rosyjska walka o Inflanty od XVI wieku. W perspektywie historycznej wpływ na współczesne relacje dwustronne mają jednak wydarzenia zdecydowanie nowsze, datujące się na wiek XVIII, XIX i XX. W wyniku traktatu w Nystad w 1721 roku Rosja przejęła od Szwecji terytoria Estonii oraz Liwonii, nad którymi panowała nieprzerwanie do 1918 roku. Mimo tak długiego okresu podporządkowania Estonia zachowała odrębność narodową, opartą w dużej mierze na związkach religijno-kulturowych z państwami nordyckimi[2]. W wyniku wojny prowadzonej w latach 1918—1920 przeciwko bolszewickiej Rosji czasowo uzyskała niepodległość, którą ponownie utraciła już w 1940 roku, kiedy stała się częścią Związku Radzieckiego. Co zrozumiałe, nie spotkało się to z zadowoleniem Estończyków, którzy w okresie II wojny światowej oraz przez pewien czas po jej zakończeniu prowadzili działania partyzanckie przeciwko władzy Kremla. Doprowadziło to do masowych represji wobec miejscowej ludności cywilnej[3].

Ze względu na proces rozpadu ZSRR Estonii udało się ponownie odzyskać suwerenność dopiero 6 września 1991 roku, co oznaczało potrzebę rozpoczęcia żmudnego procesu układania dwustronnych relacji estońsko-rosyjskich od nowa. Wpływ na nie miało kilka istotnych czynników. Przede wszystkim należy wskazać na nie najlepsze doświadczenia historyczne. Oba kraje odmiennie oceniały kluczowe wydarzenia i procesy z przeszłości, co naturalnie utrudniało możliwość nawiązania przyjaznych i partnerskich stosunków. Jak zauważył Jeroen Bult, w ciągu 20 lat okresu pozimnowojennego kontakty Rosji i Estonii niejako „utknęły" w problemach dotyczących różnych interpretacji historii. Szczególnie ostre spory rodziły wydarzenia II wojny światowej oraz represje wobec Estończyków, które nastąpiły w trakcie oraz bezpośrednio po niej[4].

Po drugie należy zwrócić uwagę na kwestię ogromnych dysproporcji potencjałów obu państw, zarówno pod względem demograficznym, geograficznym,

---

[1] W ten sposób wydarzenia te określiła np. Kertu Ruus (2008) z The European Institute.

[2] Zob. *Estonian Life*. Estonian Ministry of Foreign Affairs, Tallin 2004.

[3] *Estonia's History*. Estonia.eu: http://estonia.eu/about-estonia/history/estonias-history.html; dostęp: 16.10.2013.

[4] J. Bult: *Estonia and Russia, 20 Years on: Stuck in History*. Estonian Public Broadcasting, 25.08.2011: http://news.err.ee/politics/229ae53b-305b-4cee-9552-ae71b3f5cf90; dostęp: 16.10.2013.

gospodarczym, jak i wojskowym. Z jednej strony wiąże się to z naturalnym postrzeganiem Rosji w Tallinie jako największego zagrożenia dla narodowej niezależności. Sytuację Estonii dodatkowo utrudnia niekorzystne położenie geopolityczne pomiędzy Rosją, Łotwą a Morzem Bałtyckim, zatem jednym z głównych założeń estońskiej polityki zagranicznej po 1991 roku było odzyskanie pełnej niepodległości oraz jej zabezpieczenie[5]. Tallin pragnął osiągnąć te cele, działając w kilku kierunkach. Przede wszystkim, podobnie jak inne kraje Europy Środkowej, podjął działania obliczone na uzyskanie członkostwa w NATO i Unii Europejskiej. Estońskie elity polityczne właśnie w tych organizacjach upatrywały największej szansy na zabezpieczenie swoich interesów narodowych. Wydarzeniem, które pozwoliło na sformułowanie tego typu aspiracji, było wycofanie wojsk rosyjskich w 1994 roku. Należy ponadto wspomnieć o położeniu dużego nacisku na szybki rozwój gospodarczy oraz społeczny. W ten sposób Estonia zamierzała złagodzić narastające napięcia wewnętrzne na tle etnicznym, które potencjalnie mogły zagrozić jej bezpieczeństwu (Gerber, Conley, Moore, 2011). Można również zauważyć proces budowania bliskich związków politycznych i wojskowych z innymi państwami bałtyckimi oraz krajami nordyckimi, co było logiczne z punktu widzenia geopolitycznej sytuacji Tallina. Warto mieć przy tym świadomość, iż elity polityczne nie ukrywały wcale, że wszystkie te wysiłki wynikały głównie z zagrożenia, jakie stanowiła Rosja (zob. *National Security Concept of Estonia*, 2010: 3—9).

Z drugiej strony obszar ten spotykał się ze znacznym zainteresowaniem ze strony Kremla, ponieważ od początku lat 90. XX wieku mimo uzyskania niepodległości kraj ten zaliczano do rosyjskiej strefy wpływów. Jak słusznie zauważył Stanisław Bieleń (2006: 232):

> choć po rozpadzie ZSRR powstało 15 niepodległych państw, to jednak fakt ten nie oznaczał automatycznego zaniku wpływów Moskwy na jego dawnym obszarze. Do połowy 1993 roku przesunięto akcenty w rosyjskiej polityce zagranicznej wobec „bliskiej zagranicy". Od podejścia umiarkowanego, podkreślającego konieczność ustanowienia dobrych stosunków sąsiedzkich, opartych na wspólnych interesach, negocjacjach i kompromisie, nastąpiło przejście do polityki zdecydowanej rewindykacji. Złożyła się na to rosnąca destabilizacja na obszarze poradzieckim, nostalgia za utraconym Związkiem, a także przekonanie, że „bliska zagranica" równie silnie oddziałuje na losy rosyjskich reform, jak na stosunki z Zachodem.

Z kolei Agnieszka Bryc (2009: 51—52) stwierdziła, iż terytorium poradzieckie, a więc również Estonia, „tradycyjnie traktowane jest przez Rosję jako strefa jej żywotnych interesów, choć rozpad systemu radzieckiego na nowo

[5] *Estonian Security Policy*. Estonian Ministry of Foreign Affairs, 02.03.2011: www.vm.ee/?q=en/node/4104; dostęp: 16.10.2013.

ukształtował strefy interesów i wpływów na tym obszarze". Do najistotniejszych dla Rosji zagadnień w tym zakresie zaliczyła autorka bezpieczeństwo, rywalizację o surowce energetyczne oraz wpływ w regionie, przy czym ta druga kwestia w przypadku Estonii nie miała nigdy większego znaczenia. Zasadniczą rolę w polityce rosyjskiej wobec tego kraju, a szerzej: państw bałtyckich, odgrywały natomiast kwestie wywierania odpowiedniego wpływu, a także bezpieczeństwa. Już Andriej Kozyriew twierdził, iż na obszarze poradzieckim, w tym również w Estonii, Federacja powinna zachować „wyjątkową i uprzywilejowaną" pozycję, bardzo krytycznie postrzegano zatem wszelkie działania republik bałtyckich, których celem było oderwanie się od „rosyjskiej strefy wpływów". Aby zapobiec tym niekorzystnym procesom, prowadzono wielotorowe działania, do których należy zaliczyć za Ireneuszem Topolskim: nieudane inicjatywy integracyjne, próby zapewnienia bezpieczeństwa regionalnego, zapobieganie przejęciu przez inne republiki poradzieckie nowych technologii i strategicznych systemów uzbrojenia, powstrzymywanie obecności i wpływów państw Zachodu, uzyskanie znacznych wpływów politycznych, obecność gospodarczą, ochronę mniejszości rosyjskiej i rosyjskojęzycznej. Jak stwierdził autor, interes narodowy Federacji Rosyjskiej wymagał, aby „republiki poradzieckie prowadziły przyjazną lub w skrajnym przypadku neutralną politykę zagraniczną" (Topolski, 2013: 139—159). W przypadku Estonii szczególnie istotne znaczenie miała nie tylko ochrona mniejszości rosyjskiej, ale także powstrzymanie procesu zbliżania Tallina do Zachodu oraz polityka historyczna. Tym samym strategia Kremla wobec państw bałtyckich wpisywała się w szerszą logikę rosyjskiej mocarstwowości, którą Stanisław Bieleń (2006: 94—95) uznał nie tylko za program polityczny, lecz także pewien „rodzaj mentalności, system wartości", wywodzący się m.in. z doświadczeń historycznych.

Po trzecie zasadniczy wpływ na stosunki dwustronne w okresie pozimnowojennym wywarły kwestie demograficzne i etniczne. Ze względu na długi okres podporządkowania Rosji i ZSRR na terytorium Estonii pozostała bardzo duża grupa Rosjan. O niekorzystnych dla Estończyków procesach może świadczyć fakt, iż w 1934 roku w kraju tym żyło ok. 8% Rosjan i 4% innych narodowości (głównie Niemców i Szwedów), natomiast w latach 1945—1989 liczba osób należących do tej grupy etnicznej znacząco wzrosła, osiągając ok. 475 000 (Kirch, 2001). Ze względu na migracje z początku lat 90. na przełomie pierwszej i drugiej dekady XXI wieku populację tę oceniano na ok. 320 000, co stanowiło ok. 24,8% ogółu obywateli Estonii[6]. W tym kontekście zagadnienia te

[6] *Population and Housing Census 2011*. Statistics Estonia 2011: www.stat.ee/sdb--update?db_update_id=13545; dostęp: 15.10.2013; W. Hernád: *The Russian Minority in Estonia*. Cultural Diplomacy: www.culturaldiplomacy.org/pdf/case-studies/russian-minority.pdf; dostęp: 15.10.2013; R. Lokk: *The Russian Minority in Post-Communist Estonia. A Comparison with Czech-Sudeten German Relations*: www.stm.unipi.it/clioh/tabs/libri/9/15-Lokk_217-240.pdf; dostęp: 15.10.2013.

tworzyły od początku nie lada wyzwanie dla rządu w Tallinie. Ryzyko pojawienia się napięć na tle etnicznym stanowiło jeden z najistotniejszych determinantów estońskiej polityki zagranicznej, obliczonej na integrację z zachodnimi strukturami bezpieczeństwa. Kwestie te wywierały również niekorzystny wpływ na estońską politykę wewnętrzną ze względu na częste utożsamianie się ludności rosyjskiej z interesami Federacji, dostrzegano zatem możliwość ingerencji Kremla w wewnętrzne sprawy państwa. Problem ten był tym większy, iż, jak wspomniano wyżej, Moskwa była żywotnie zainteresowana ochroną ludności rosyjskojęzycznej w Estonii (Szyszłak, 2011). Ireneusz Topolski (za Aleksiejem Arbatowem) pisał w tym kontekście, że zapewnienie praw etnicznych Rosjan mieszkających na obszarze poradzieckim ma fundamentalne znaczenie i jest jej „świętym obowiązkiem". Jego zdaniem sprawia to, iż „Federacja jest zobowiązana do reagowania na polityczne i kulturalne postulaty diaspory rosyjskiej i ludności rosyjskojęzycznej […], problemy związane z naruszaniem ich praw i interesów, w tym m.in. przejawów dyskryminacji, przekładają się na relacje Federacji z byłymi republikami" (Topolski, 2013: 155).

Na tym tle relacje rosyjsko-estońskie od momentu rozpadu Związku Radzieckiego miały dość burzliwy charakter. Początek lat 90. XX wieku był przede wszystkim zdeterminowany próbami podporządkowania politycznego Estonii przez Kreml i zablokowania jej prozachodnich aspiracji. Wiązało się to z odwołaniem do takich środków, jak odcinanie dostaw gazu, sankcje gospodarcze czy ostre polemiki polityczne związane z polityką Tallina wobec mniejszości rosyjskiej[7]. Sytuację dodatkowo komplikował fakt stacjonowania w tym kraju do 1994 roku wojsk FR (Made, 2005: 94—95). Dopiero po ich wyprowadzeniu Estonia uzyskała realne możliwości ubiegania się o członkostwo w strukturach Paktu Północnoatlantyckiego i Unii Europejskiej, co jednak nadal budziło dwustronne napięcia. Do pewnego odprężenia doszło dopiero w drugiej połowie lat 90., kiedy Estonia została formalnie zaproszona do UE, a Rosja zawarła porozumienie z Sojuszem Północnoatlantyckim. Mimo pozornego zaakceptowania prozachodniego kursu polityki estońskiej wzajemne relacje na przełomie wieków pozostały chłodne (Ibidem, s. 93).

Do wzrostu znaczenia Estonii w polityce zagranicznej Rosji doszło naturalnie w 2004 roku, wraz z uzyskaniem przez nią członkostwa w UE i NATO. Jak zauważyli eksperci Center for Strategic & International Studies, Kreml zaczął się wówczas odwoływać do bardziej subtelnych instrumentów nacisku, takich jak środki propagandowe, których celem było zdyskredytowanie młodej republiki na arenie międzynarodowej oraz zmiana jej wizerunku jako modelowego przykładu transformacji na obszarze poradzieckim. Zdecydowanie więk-

[7] Znaczne kontrowersje wywoływał np. fakt, iż wielu etnicznych Rosjan nie mogło uzyskać estońskiego obywatelstwa. Zob. *Annual Report: Estonia 2013*. Amnesty International, 23.05.2013: www.amnestyusa.org/research/reports/annual-report-estonia-2013; dostęp: 15.10.2013.

szy nacisk położono na zagadnienia związane z ochroną mniejszości rosyjskiej w Estonii oraz z zagadnieniami historycznymi. Ostrą krytykę ze strony Moskwy budziły estońskie ustawodawstwo dotyczące języka oraz wymogi uzyskania obywatelstwa, co jej zdaniem dyskryminowało Rosjan. W związku z tym Federacja zaczęła aktywnie pomagać tej grupie, zarówno politycznie, jak i humanitarne, przy wykorzystaniu organizacji pozarządowych oraz rosyjskojęzycznych mediów. Stopniowo coraz większe napięcia budziły również odmienne interpretacje wydarzeń historycznych (Conley, Gerber, Moore, David, 2011: 1—4). W tym czasie zaszły również zmiany w estońskiej polityce zagranicznej wobec Rosji: wraz z akcesją do UE i NATO Tallin zaczął stopniowo ograniczać kontakty dwustronne na rzecz większego zaangażowania w nie struktur zachodnich. Wynikało to ze świadomości, iż zabezpieczenie interesów narodowych będzie możliwe jedynie przy wsparciu całego potencjału Unii Europejskiej. Skuteczność tego rodzaju instrumentów w polityce zagranicznej Estonii okazała się jednak ograniczona (Made, 2005: 93—107).

W drugiej połowie pierwszej dekady XXI wieku napięcia na tle historycznym i narodowościowym w Estonii zogniskowały się przede wszystkim na posągu tzw. Brązowego Żołnierza w Tallinie. Odsłonięty w 1947 roku monument miał być przede wszystkim hołdem dla radzieckich żołnierzy poległych w walkach na terenie tego kraju. Wśród Estończyków pomnik ten zawsze wywoływał kontrowersje, przypominając o utraconej suwerenności i stratach poniesionych w wyniku zajęcia przez ZSRR. Szczególnie mocno problemy na tym tle narosły właśnie w okresie pozimnowojennym. Z jednej strony Brązowy Żołnierz stał się niejako symbolem radzieckiej okupacji kraju, przez co pojawiły się pomysły jego przeniesienia w inne, mniej eksponowane miejsce. Z drugiej jednak strony posąg ten zyskał zasadnicze znaczenie dla mniejszości rosyjskiej, która uznała go za najważniejszy monument Estonii, przypominający zwycięstwo nad nazizmem oraz poświęcenie żołnierzy ZSRR. Jako że kwestią jego przeniesienia zainteresowały się estońskie elity polityczne, doprowadziło to do narastającego wewnętrznego kryzysu politycznego. W 2006 roku konserwatywna partia Pro Patria (*Isamaaliit*) zwróciła się do władz miejskich w Tallinie o jego zniszczenie, co doprowadziło do pierwszych starć ulicznych między estońskimi nacjonalistami a rosyjską mniejszością. Sprzeciwił się temu prezydent Toomas Hendrik Ilves, który nakazał jego przeniesienie z centrum miasta. Reakcją na to były kolejne zamieszki, którymi zainteresowały się w końcu media i elity polityczne Federacji Rosyjskiej[8]. Jak tłumaczył później estoński minister obrony Jaak Aaviksoo, statua musiała zniknąć ze względu na gloryfikację totalitarnego reżimu, jakim był Związek Radziecki. Jego zdaniem rosyjska mniejszość, która

[8] *Estonia to remove Soviet memorial*. BBC NEWS, 12.01.2007: http://news.bbc.co.uk/2/hi/europe/6255051.stm; dostęp: 18.10.2013; *Estonian nationalists attempt to vandalise monument*. RT.com, 23.02.2007: http://rt.com/news/estonian-nationalists-attempt-to-vandalise-monument; dostęp: 18.10.2013.

zbierała się pod pomnikiem, manifestowała swoje poparcie dla dorobku ZSRR, wielokrotnie zmuszając demonstrujących Estończyków do ustąpienia. Odrzucił także oskarżenia o dyskryminację Rosjan, twierdząc, iż po prostu odebrano im przywileje, którymi cieszyli się przed 1991 rokiem[9].

Narastające napięcia wokół Brązowego Żołnierza wpisały się w odbywające się w Estonii w marcu 2007 roku wybory parlamentarne, w których ponownie zwyciężyła partia Andrusa Ansipa. Umożliwiono w nich obywatelom oddanie głosu za pomocą Internetu, co stanowiło innowację na skalę światową. W innych państwach zdarzało się to dotychczas jedynie w wyborach lokalnych. W sumie z możliwości tej skorzystało 30 275 Estończyków (zob. Treschel, 2007). Fakt ten świadczył najlepiej o ogromnym znaczeniu technologii informatycznych w tym kraju. W tym kontekście Vincent Joubert (2012: 1) pisał:

> Estonia, jakkolwiek jedno z najmniejszych państw NATO, jest jednym z najbardziej zaawansowanych technologicznie krajów świata. Niemal każda działalność [jest tam — M.L.] dokonywana za pomocą Internetu, począwszy od osobistych transakcji bankowych, aż po edukację, dostęp do mediów czy uczestnictwo w wyborach lokalnych.

Dzięki zdecydowanemu przyspieszeniu w tej dziedzinie od przełomu XX i XXI wieku osiągnięcia rewolucji informatycznej zaczęły być tam stosowane masowo zarówno w wymiarze społecznym, jak i państwowym. Najlepiej świadczą o tym dane, według których w 2012 roku ponad 78% populacji i 75% gospodarstw domowych miało stały dostęp do Internetu. Dzięki coraz powszechniejszemu wykorzystaniu technologii informacyjnych i komunikacyjnych od początku wieku estońskie władze rozpoczęły działania zmierzające do realizacji koncepcji e-państwa. W skrócie oznaczało to ułatwienie obywatelom kontaktu ze wszystkimi szczeblami administracji państwowej oraz wieloma elementami sektora prywatnego za pomocą sieci. W praktyce przejawiało się to m.in. możliwością edukacji (*e-kool*), rozliczania podatków czy uzyskania państwowego adresu e-mail połączonego z elektronicznym dowodem osobistym. Jeśli chodzi o sektor prywatny, to należy podkreślić ogromną popularność bankowości elektronicznej, z której korzystała zdecydowana większość obywateli (ponad 99% transakcji było dokonywanych online). W sumie społeczeństwo Estonii w 2012 roku miało dostęp do ok. 2500 internetowych usług sektora publicznego i prywatnego[10]. Wszystkie powyższe dane wskazują, iż Estonia przełomu pierwszej i drugiej dekady XXI wieku była krajem wyjątkowym pod względem stopnia zaawansowania rewolucji informatycznej. Żadne inne państwo obszaru pora-

[9] *Estonia: Defense Minister Says Bronze Soldier Had To Go*. Radio Free Europe, 09.05.2007: www.rferl.org/content/article/1076363.html; dostęp: 18.10.2013.

[10] *Facts about e-Estonia*. Estonian Information System's Authority: www.ria.ee/facts--about-e-estonia; dostęp: 18.10.2013.

dzieckiego, a nawet Europy Środkowej nie czerpało tak szeroko z potencjału technologii informacyjnych i komunikacyjnych. Z tym wiązał się jednak swoisty paradoks bezpieczeństwa, którego w porę nie dostrzeżono, wraz z postępującym uzależnieniem od komputerów i sieci nie zwrócono bowiem należytej uwagi na fakt, iż oznaczało to zarazem zwiększoną wrażliwość na ataki w cyberprzestrzeni (zob. Stanley, 2010). Było to oczywiście na rękę Moskwie. Z jednej strony pozornie Rosja była zapóźniona pod względem wdrażania najnowszych technologii teleinformatycznych w życiu gospodarczym czy społecznym, z drugiej jednak już w roku 2000 przyjęto tam doktrynę bezpieczeństwa informacyjnego, zakładającą podnoszenie zdolności w tej dziedzinie. Także poszczególni przedstawiciele Kremla od przełomu XX i XXI wieku coraz częściej wspominali o potrzebie przygotowania się do ewentualnego konfliktu w cyberprzestrzeni (Bógdał-Brzezińska, Gawrycki, 2003: 201—213). Wskazywało to więc wyraźnie, iż Federacja od dawna budowała swój potencjał do działań w środowisku teleinformatycznym.

Na tle omówionych wyżej procesów i wydarzeń w kwietniu 2007 roku rząd Estonii podjął ostatnie przygotowania do usunięcia pomnika z centrum Tallina. Doprowadziło to do narastających napięć między siłami porządkowymi a rosyjską mniejszością, co w konsekwencji przekształciło się w masowe zamieszki. Rozpoczęły się one na pełną skalę 26 kwietnia w trakcie przygotowań do operacji przeniesienia posągu. Do incydentów doszło również w innych częściach kraju, gdzie zaczęto niszczyć pomniki estońskich bohaterów wojennych. W sumie w ciągu ponaddwudniowych walk ulicznych, w których brało udział ok. 3000 osób, zginął jeden protestujący Rosjanin, 153 osoby zostały ranne, a przeszło 800 aresztowano[11]. Wydarzenia w Estonii wywołały ogromną krytykę ze strony rosyjskich mediów oraz rządu. Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej oskarżyło rząd w Tallinie o nadmierne stosowanie siły wobec protestujących oraz obrazę wszystkich, którzy walczyli podczas II wojny światowej z nazizmem. Siergiej Ławrow ostrzegł wówczas, iż Kreml podejmie „poważne kroki" w odpowiedzi na usunięcie monumentu oraz działania sił bezpieczeństwa. Domagano się również pełnej informacji na temat zabitego Rosjanina. Temat ten poruszono w rozmowie telefonicznej między Władimirem Putinem a Angelą Merkel[12]. W listopadzie 2007 roku wątpliwości dotyczące reakcji Estonii wyraził również Komitet Przeciwko Torturom ONZ (*Consideration of Reports*, 2007). Warto także wspomnieć, iż 30 kwietnia 2007 roku przebywająca

[11] *Tallin tense after deadly riots*. BBC News, 28.04.2007: http://news.bbc.co.uk/2/hi/europe/6602171.stm; dostęp: 18.10.2013; *The Last Soviet in Tallin: Saga of the 'Bronze*… Local Life: www.local-life.com/tallinn/articles/estonian-russian-relations; dostęp: 18.10.2013.

[12] *Moscow Says Russian Killed During Tallin Riots*. Radio Free Europe, 28.04.2007: www.rferl.org/content/article/1076165.html; dostęp: 18.10.2013; N. Adomaitis, *Estonia calm after Red Army site riots*. Reuters, 29.04.2007: http://uk.reuters.com/article/2007/04/29/uk-estonia-russia-idUKL2873034620070429; dostęp: 18.10.2013.

z wizytą w Tallinie delegacja rosyjskiej Dumy wezwała rząd estoński do dymisji w związku z tymi wydarzeniami (zob. *Estonia vs. Russia*, 2007).

Rezultat powstałego kryzysu politycznego okazał się zaskoczeniem nie tylko dla Estończyków, ale i całego świata. Już 26 kwietnia w trakcie najbardziej natężonych walk ulicznych w Tallinie rozpoczęła się kampania zmasowanych cyberataków wymierzonych zarówno w sektor publiczny, jak i prywatny, która zakończyła się dopiero 18 maja 2007 roku (zob. Richards, 2009; Lesk, 2007). Analitycy podzielili ją na kilka faz. Pierwsza miała prawdopodobnie charakter czysto spontaniczny, w którym internauci popierający mniejszość rosyjską zaczęli samoistnie organizować się w sieci. Zarówno wyspecjalizowani haktywiści patriotyczni, jak i zwykli *script kiddies*, dzięki forom internetowym, blogom oraz innym witrynom poświęconym hakingowi zdołali zainicjować pierwsze stosunkowo nieskomplikowane cyberataki typu DDoS przeciwko władzom Estonii. Na cel wzięto wówczas głównie strony rządowe, stosując do tego proste programy i komendy rozpowszechniane w rosyjskim Internecie. Drugi etap kampanii rozpoczął się pod koniec kwietnia, kiedy, jak zauważył Dimitar Kostadinov, zaczęły się one charakteryzować coraz większym stopniem zaawansowania. Wówczas zaczęto stosować na dużą skalę wielkie sieci *botnet*, które towarzyszyły prostszym metodom wykorzystywanym przez rosyjskich *script kiddies* i haktywistów. Do kolejnego, zdecydowanie groźniejszego w skutkach natężenia incydentów teleinformatycznych doszło w dniach 3—4 maja, kiedy wzięto na cel usługi i strony sektora prywatnego, w tym przede wszystkim krajowych banków. Do kulminacji tej kampanii doszło jednak dopiero w nocy 9 maja, w rocznicę zwycięstwa Związku Radzieckiego nad hitlerowskimi Niemcami. W tej trwającej trzy dni fazie skupiono się ponownie na sektorze finansowym[13]. Sygnałem do rozpoczęcia cyberataków stała się wypowiedź Władimira Putina w trakcie parady wojskowej na Placu Czerwonym, który potępił tych, którzy „bezczeszczą pomniki bohaterów wojennych"[14]. Wówczas w rosyjskim Internecie pojawiły się setki wiadomości, w których nawoływano do partycypacji w atakach. W jednej z nich użytkownik Victoris pisał na forum dyskusyjnym: „Nie zgadzasz się z polityką eSStoni? […] Myślisz, że nie masz wpływu na sytuację??? MOŻESZ go mieć w Internecie!" (Davis, 2007). O skali tych incydentów mogły świadczyć dane przytoczone przez „Wired", według których liczba pakietów danych przesyłanych z zagranicy do Estonii w nocy z 8 na 9 maja zwiększyła się 200-krotnie w stosunku do stanu normalnego (Ibidem). Główną ofiarą stał się wówczas największy bank Estonii Hansabank, któ-

[13] J. Wiebke: *Cyber Warfare. Case Study: Estonia*. 05.04.2012: www.personal.utulsa.edu/~james-childress/cs5493/Present2012/Wiebke.pdf; dostęp: 18.10.2013; D. Kostadinov: *Estonia: To Black Out an Entire Country — part one*. INFOSEC Institute, 01.10.2013: http://resources.infosecinstitute.com/estonia-to-black-out-an-entire-country-part-one; dostęp: 18.10.2013.

[14] *Putin in veiled attack on Estonia*. BBC News, 09.05.2007: http://news.bbc.co.uk/2/hi/europe/6638029.stm; dostęp: 21.10.2013.

remu nie tylko zablokowano możliwość świadczenia usług online, ale także odcięto go od zagranicznych sieci bankowych, skutkiem czego Estończycy czasowo stracili możliwość korzystania z kart bankomatowych[15]. Kolejne poważniejsze incydenty miały miejsce 15 maja, kiedy do cyberataków wykorzystano sieć *botnet* liczącą ok. 85 000 komputerów. Tym razem ponownie na cel zostały wzięte estońskie instytucje państwowe, jednak dzięki prawidłowej reakcji zespołu CERT udało się zapobiec poważniejszym szkodom. Ostatnia fala nastąpiła 18 maja, lecz i tym razem estońskim informatykom udało się zapobiec paraliżowi rządowych stron internetowych[16]. Analitykom w większości przypadków nie udało się ustalić sprawców, którzy skutecznie maskowali swoją tożsamość, m.in. wykorzystując komputery zlokalizowane w państwach zachodnich.

Wyjątkowość omówionych wyżej wydarzeń polegała przede wszystkim na ich masowości. W przeciwieństwie do wcześniejszych incydentów tego typu w cyberatakach owych brały udział od początku setki tysięcy komputerów, przez co ich zablokowanie nie było łatwe. W tym kontekście warto więc szerzej omówić ich właściwości techniczne. Według danych węgierskiego zespołu CERT (Hun-CERT) pochodzących z systemu ATLAS[17] między 27 kwietnia a 11 maja 2007 roku doszło w sumie do 128 unikalnych ataków metodą *Distributed Denial of Service*, z czego 115 z wykorzystaniem techniki *ICMP flood* (inaczej *ping flood* albo *smurf attack*), a 4 za pomocą *TCP SYN flood*. Z tego 35 było wymierzonych w witrynę internetową policji (www.pol.ee), 7 parlamentu (www.riigikogu.ee), 36 portalu *Gateway to eEstonia* (www.eesti.ee), rządu (www.peaminister.ee, www.valitsus.ee), 2 w Ministerstwo Polityki Społecznej (www.sm.ee), 2 w Ministerstwo Ochrony Środowiska (www.envir.ee), 6 w Ministerstwo Rolnictwa (www.agri.ee) i aż 35 w Ministerstwo Finansów (www.fin.ee). Czas trwania większości oscylował w granicach 1 godziny, jednak aż piętnaście z nich trwało powyżej pięciu godzin (w tym 10 i więcej). O dużej skali ataków świadczył fakt, iż przepustowość części z nich docierała do granicy 90 Mb/s. W większości stały za nimi nie tylko rozwinięte sieci *botnet*, ale także mniej zaawansowane narzędzia, udostępniane na stronach rosyjskich haktywistów (np. www.zyklonteam.org). Ochotników do tego typu działań zbierano także na forach niezwiązanych bezpośrednio z hakingiem. Dzięki nim niemal każdy internauta mógł stosunkowo łatwo uzyskać wyspecjalizowane środki przydatne do ataków na estońską sieć[18].

Ponadto niemal od początku masowym atakom DDoS towarzyszyły częste przypadki *web defacement*, czyli podmiany zawartości stron internetowych. Nie

[15] Richards, 2009; Kostadinov, op.cit.

[16] Kostadinov, op.cit.

[17] Szerzej na temat systemu ATLAS w Nazario, 2009.

[18] B. Toth: *Estonia under cyber attack*. Hun-CERT, s. 1—3: www.cert.hu/sites/default/files/Estonia_attack2.pdf; dostęp: 18.10.2013.

tylko zamieszczano na nich sowieckie i rosyjskie materiały propagandowe, lecz również spreparowane przeprosiny estońskiego rządu dla Rosjan (Geers, 2008: 9). Wykorzystywano do tego głównie metodę *SQL injection*[19]. Prawdopodobnie po raz pierwszy włamano się w ten sposób na stronę domową ministra spraw zagranicznych Urmasa Paeta, gdzie opublikowano wizerunek radzieckiego żołnierza z napisem *Zwycięstwo Dziadka moim zwycięstwem*. Niedługo później zaczęto w ten sposób atakować strony wszystkich ministerstw estońskich za wyjątkiem ministerstwa kultury oraz rolnictwa[20].

Jeśli chodzi o inne metody stosowane w trakcie tzw. „pierwszej cyberwojny", to należy wspomnieć również o ogromnej ilości e-maili i spamu. Wszystkie komentarze i wiadomości zamieszczane wówczas w sieci miały charakter *stricte* propagandowy, obliczony na sparaliżowanie normalnej dyskusji online i zemstę na obywatelach Estonii. W niezwykły sposób wykorzystano także unikalną otwartość rządu tego kraju na kontakty z internautami. Ze względu na fakt, iż adresy poczty elektronicznej wszystkich urzędników państwowych były publicznie znane, codziennie zasypywano je tysiącami wiadomości w nadziei na ich zablokowanie[21].

Warto również zastanowić się nad kierunkami cyberataków przeciwko Estonii. Pierwszymi i najbardziej oczywistymi były strony władzy ustawodawczej i wykonawczej, a także witryny domowe oraz konta e-mail najważniejszych polityków. W zasadzie przez całą kampanię były one przedmiotem zmasowanych cyberataków. Co jednak zdecydowanie ważniejsze, poważnym obiektem zainteresowania sprawców był sektor prywatny. Atakowano pojedynczych użytkowników oraz strony domowe. Włamywano się również na portale największych estońskich mediów, a także przedsiębiorstw budowlanych i telekomunikacyjnych, zamieszczając tam materiały propagandowe. W ten sposób zamieniono np. zawartość witryny działającego w Tallinie dewelopera Siilimaja, na której pojawiła się radziecka czerwona gwiazda z napisem *Our Freedom, Our Victory*[22]. Zainteresowano się także wybranymi elementami infrastruktury teleinformatycznej, o czym świadczyło wzięcie na cel największych estońskich banków. Było to o tyle bolesne, iż, jak wspomniano, bankowość elektroniczna była w Estonii niezwykle popularną usługą. Po 1 maja zaatakowani zostali również najwięksi dostawcy usług internetowych, co miało prowadzić do zakłócenia funkcjonowania krajowej sieci. W niektórych raportach wspominano wręcz, iż doszło do uszkodzenia niektórych routerów[23]. Ponadto czasowo zablokowano funkcjono-

[19] Kostadinov, op.cit.

[20] Zob. Toth, op.cit.

[21] Kostadinov, op.cit.

[22] *Estonia Cyber Attacks 2007.* Afrinic.net: http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf; dostęp: 21.10.2013; B. Toth: *Estonia under cyber attack*. Hun-CERT, s. 4: www.cert.hu/sites/default/files/Estonia_attack2.pdf; dostęp: 18.10.2013

[23] *Estonia Cyber Attacks 2007*, op.cit.

wanie numeru alarmowego 112, w związku z czym obywatele przez pewien czas nie mieli dostępu do służb ratunkowych. Powyższe przykłady pozwalają stwierdzić, iż doszło do naruszenia bezpieczeństwa infrastruktury krytycznej Estonii. Niektórzy eksperci zwrócili jednak uwagę, że cyberataki starannie omijały najważniejsze jej elementy, takie jak sieć elektroenergetyczna czy transportowa[24]. Można więc uznać, iż sprawcy nie chcieli poczynić poważniejszych szkód, lecz uzyskać określone efekty w wymiarze politycznym.

Dopiero w trzy dni po pierwszych cyberatakach służby Estonii zdecydowały się na bardziej zorganizowaną reakcję, blokując wszystkie domeny z rozszerzeniem .ru. Działania te okazały się jednak nieskuteczne, gdyż utrudniły aktywność tylko tych sprawców, którzy wykorzystywali wspomniane już, mało zaawansowane oprogramowanie do prowadzenia DDoS z terytorium Federacji. Najpoważniejsze cyberataki opierały się natomiast na potencjałach wielu wynajętych sieci *botnet*, liczących w sumie nawet do miliona komputerów z całego świata, w tym m.in. ze Stanów Zjednoczonych, Chin, Wietnamu czy Peru. W związku z tym władze w Tallinie zdecydowały się poprosić o pomoc instytucje międzynarodowe. Przede wszystkim zwrócono się do Sojuszu Północnoatlantyckiego, który nie miał jednak wypracowanych mechanizmów reagowania na tego typu sytuacje. Zdecydowano się w końcu na wysłanie dwóch specjalistów komputerowych NATO, do których dołączył jeszcze trzeci ekspert z USA. Niestety, nie przyczynili się oni w większym stopniu do zwiększenia skuteczności służb estońskich. O pomoc poproszono również stowarzyszenie TERENA (Trans-European Research and Education Networking Association), które zdecydowało się na jej udzielenie przy wykorzystaniu Computer Security Incident Response Teams. Niestety, zaczęły one działać stosunkowo późno, dopiero od 3 maja 2007 roku[25]. Ograniczonego wsparcia udzielił również doświadczony w tej dziedzinie Izrael (Saleem, Hassan, 2009: 2). Warto także wspomnieć, iż estońscy internauci podjęli pewne ograniczone próby rewanżu. Obejmowały one włamania na stosunkowo mało istotne rosyjskie strony WWW i zmianę zawartości, w tym: www.web-dozor.ru czy www.1-net.ru, gdzie zamieszczano hasła typu *Estonia forever* czy *Proud to be Estonian*[26].

Omówione wydarzenia spotkały się z ogromnym zainteresowaniem międzynarodowej opinii publicznej, po raz pierwszy w historii suwerenny kraj stał się bowiem obiektem zmasowanych cyberataków na taką skalę. Zachodnie media zaczęły się prześcigać w raportach na ten temat, zamiennie stosując terminy *cyberwojny* i *cyberterroryzmu*. Do tego pierwszego pojęcia odwoływały się m.in. artykuły w „The New York Times", „The Guardian" (*Russia*

[24] J. Wiebke: *Cyber Warfare. Case Study…*, op.cit.; D. Kostandinov: *Estonia: To Black Out an Entire Country — part two*. INFOSEC Institute, 08.10.2013: http://resources.infosecinstitute.com/estonia-to-blackout-an-entire-country-part-2; dostęp: 21.10.2013.

[25] Toth, op.cit., s. 5.

[26] Toth, op.cit., s. 6.

accused to unleashing cyberwar to disable Estonia) oraz na stronie internetowej BBC (*Estonia hit by 'Moscow cyber war'*). Większość z nich oceniała, że incydenty te stanowiły poważne zagrożenie bezpieczeństwa narodowego Estonii. Co więcej, uznano, iż kraj ten otarł się o zupełny paraliż „infrastruktury cyfrowej" (za: Farivar, 2009: 182—188). Z kolei o cyberterroryzmie pisały m.in. „The Telegraph", Dailymail.co.uk czy Yahoo.com[27]. W większości przypadków, na co zwrócił uwagę m.in. Kevin Poulsen z „Wired", w alarmistycznym tonie pisano o możliwym „cyberarmageddonie"[28]. Z jednej strony media masowe w sposób nadmiernie uproszczony i pozbawiony głębszej refleksji charakteryzowały przebieg wydarzeń w Estonii, z drugiej jednak prawidłowo dostrzegły ich doniosłe znaczenie jako nowej formy zagrożeń bezpieczeństwa narodowego i międzynarodowego.

W tym kontekście od samego początku pojawiały się wątpliwości, w jaki sposób należy interpretować te incydenty, zarówno z punktu widzenia stosunków estońsko-rosyjskich, zasad funkcjonowania Sojuszu Północnoatlantyckiego, praktyki współpracy w ramach Organizacji Narodów Zjednoczonych, jak i wykładni prawa międzynarodowego publicznego. Scott J. Schackelford (2009: 211) pisał, iż w ujęciu prawnym istniały dwie możliwe reakcje na tego typu wydarzenia. Zgodnie z jedną cyberprzestrzeń mogła być uznana przez społeczność międzynarodową za domenę, w której państwa mogą skutecznie egzekwować suwerenność, według drugiej natomiast sfera ta mogła zostać potraktowana w sposób podobny do wspólnego dziedzictwa ludzkości. W obu przypadkach wiązało się to z doniosłymi konsekwencjami dla prawa międzynarodowego. Sytuacja ta była tym bardziej skomplikowana, że działania prowadzone w cyberprzestrzeni rodziły omówione już problemy z identyfikacją pomysłodawców, organizatorów oraz bezpośrednich sprawców tych cyberataków. Mimo to rząd w Tallinie, uznając je za naruszenie bezpieczeństwa narodowego, wskazywał jednoznacznie na winę Kremla. Jak zauważył premier Estonii Andrus Ansip, był to pierwszy przypadek w historii, kiedy niepodległy kraj został zaatakowany na taką skalę przez Internet. Jego zdaniem „na Estonii testowano nowy model wojny cybernetycznej", w której paraliż stron WWW był porównywalny z blokadą portów i lotnisk. W innej wypowiedzi twierdził: „cyberataki [pochodzące — M.L.] z rosyjskich serwerów rządowych wraz ze zniszczeniem estońskiej

[27] A. Hanlon: *Attack of the cyber terrorists*. Mail Online, 24.05.2007: www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html; dostęp: 21.10.2013; A. Blomfield: *Russia accused over Estonian 'cyber-terrorism'*. „The Telegraph", 17.05.2007: www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html; dostęp: 21.10.2013; *Cyber-terrorism Has Become a Reality - The Russia-Estonia Cyber-Terrorism Face Off*. Yahoo.com, 15.06.2007: http://voices.yahoo.com/cyber-terrorism-has-become-reality-russia-estonia-391715.html; dostęp: 21.10.2013.

[28] K. Poulsen: *'Cyberwar' and Estonia Panic Attack*. „Wired" 22.08.2007: www.wired.com/threatlevel/2007/08/cyber-war-and-e; dostęp: 21.10.2013.

flagi z naszej ambasady oraz wypowiedziami polityków rosyjskiej Dumy wzywających do zmiany rządu w Estonii wskazują, że nasze niepodległe państwo zostało poważnie zaatakowane"[29]. Minister obrony Jaak Aaviksoo wskazał natomiast, że incydenty te stanowiły poważny problem dla całego Sojuszu Północnoatlantyckiego, gdyż nie uznawał on dotychczas cyberataków za akcje o charakterze militarnym[30]. Z kolei minister spraw zagranicznych Estonii Urmas Paet, w wywiadzie dla „The Times" stwierdził:

> jeśli ataki pochodzą z oficjalnych adresów IP rosyjskiego rządu i nie tylko dotykają naszych stron internetowych, ale także naszych sieci telefonii komórkowej i sieci usług ratowniczych, wtedy jest to […] bardzo groźne. […] To może kosztować życie […]. Większa część tych ataków pochodzi z Rosji i z oficjalnych serwerów jej rządu[31].

Warto także przytoczyć słowa rzecznika estońskiego Ministerstwa Obrony Madisa Mikko, który porównał incydenty teleinformatyczne do konwencjonalnych operacji zbrojnych: „Jeśli dochodzi do ataku rakietowego, na, powiedzmy, lotnisko, to jest to akt wojny. […] Jeśli ten sam rezultat został osiągnięty przez komputery, to jak inaczej można ocenić tego rodzaju atak?"[32]. Należałoby także wspomnieć o wypowiedzi ambasador Estonii w Moskwie Mariny Kaljurand, według której zarówno cyberataki, jak i zamieszki w Tallinie były inspirowane i sterowane z Kremla[33]. W związku z taką interpretacją wydarzeń rząd Estonii zwołał posiedzenie ministrów obrony państw NATO poświęcone tej sprawie. Rzecznik Organizacji Robert Pszczel odniósł się ze zrozumieniem do stanowiska Tallina, twierdząc: „Dziś Estonia, jutro może być to ktoś inny"[34]. W efekcie Sojusz Północnoatlantycki, który okazał się bezradny wobec masowych cyberataków na państwo członkostwie, dość szybko podjął działania naprawcze. Jak stwierdził Vincent Joubert (2012: 1), był to więc swoisty „ostatni dzwonek", który w praktyce udowodnił organizacji, jakie mogą być skutki masowej kampanii w cyberprzestrzeni. Już 14 czerwca 2007 roku eksperci NATO zaprezentowali raport na temat tych wydarzeń, który stał się podstawą przyszłych reform.

---

[29] Za: Lakomy, 2010b: 61; N. Anderson: *Massive DDoS attacks target Estonia; Russia accused*. Ars Technica, 14.05.2007: http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused; dostep: 18.10.2013.

[30] Ibidem.

[31] A. Bright: *Estonia accuses Russia of 'cyberattack'*. „The Christian Science Monitor" 17.05.2007: www.csmonitor.com/2007/0517/p99s01-duts.html; dostęp: 18.10.2013.

[32] *Russia: Monument Dispute With Estonia Gets Dirty*. Radio Free Europe, 04.05.2007: www.rferl.org/content/article/1076297.html; dostęp: 21.10.2013.

[33] Ibidem.

[34] S.L. Myers: *Cyberattack on Estonia stirs fear of 'virtual war'*. „The New York Times" 18.05.2007: www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html?_r=0; dostęp: 21.10.2013.

Z punktu widzenia Estonii najważniejszą reakcją było powołanie w maju 2008 roku w Tallinie Centrum Doskonalenia Cyberobrony[35]. Na tym tle warto zaznaczyć, iż zdecydowanie odmienną optykę tych incydentów przyjął Kreml. Ostro krytykując rząd Ansipa za politykę antyrosyjską, jednocześnie odciął się od odpowiedzialności za cyberataki. 17 maja 2007 roku rzecznik Kremla Dmitrij Pieskow określił te zarzuty mianem „absolutnego kłamstwa". Zauważył przy tym, że strona internetowa prezydenta Rosji jest atakowana setki razy dziennie, za zatem zgodnie z logiką Tallina oznaczałoby to odpowiedzialność innych rządów za te incydenty[36].

Prawidłowa ocena istoty i prawnomiędzynarodowych skutków trzytygodniowej kampanii cyberataków w Estonii zależała przede wszystkim od identyfikacji winowajców. Jak wspomniano wyżej, na tym tle pojawiły się jednak dość poważne rozbieżności, ponieważ sprawcy dzięki umiejętnemu wykorzystaniu potencjału cyberprzestrzeni w zdecydowanej większości przypadków byli w stanie ukryć swoją tożsamość. Na podstawie dostępnych informacji formułowano więc zgoła odmienne opinie na ten temat (Willson, 2012: 25). Część komentatorów wskazywała jednoznacznie, iż nie miały one charakteru „cyberwojny". Bliżej im było natomiast do pewnych „cyberzamieszek", w których brali udział patriotycznie nastawieni internauci (haktywiści patriotyczni). Ich zdaniem wszystkie cechy tych ataków wskazywały, iż nie były one zorganizowaną akcją przeprowadzoną przez władze państwowe. Miał o tym świadczyć m.in. fakt, iż na rosyjskich blogach organizowano zbiórki pieniędzy na wynajem sieci *botnet*[37]. W analizie Muhammada Saleema i Jawada Hassana stwierdzono z kolei, iż cyberataki w tym wydaniu stanowiły raczej „broń masowego zakłócania", a nie zniszczenia (Saleem, Hassan, 2009: 6). W podobny sposób sprawę tę postrzegał fiński ekspert Mikko Hyppönnen, który podkreślił, iż incydenty te nie przeistoczyły się w cyberwojnę[38]. Tego typu opinie współgrały z deklaracją jednego z przywódców młodzieżowej prokremlowskiej organizacji Nasi Konstantina Goloskowa, który 2 maja 2007 roku w rozmowie z agencją Rosbalt

[35] S. Myrli: *NATO and Cyber Defense*. NATO Parliamentary Assembly, 173 DSCFC 09 E BIS; *Cooperative Cyber Defence Centre of Excellence*: www.ccdcoe.org; dostęp: 21.10.2013.

[36] *Kremlin denies involvement in cyber attacks on Estonia*. „The Baltic Times" 18.05.2007: www.baltictimes.com/news/articles/17908; dostęp: 21.10.2013.

[37] Zob. np. B. Brenner: *Black Hat 2007: Estonian attacks were a cyber riot, not warfare*. SearchSecurity, 03.08.2007: http://searchsecurity.techtarget.com/news/1266728/Black-Hat-2007-Estonian-attacks-were-a-cyber-riot-not-warfare; dostęp: 18.10.2013; L. Greenemeier: *Estonian 'Cyber Riot' Was Planned, But Mastermind Still A Mystery*. „Information Week" 03.08.2007: www.informationweek.com/estonian-cyber-riot-was-planned-but-mast/201202784; dostęp: 18.10.2013.

[38] C. Boyd: *Cyber-war a growing threat warn experts*. BBC News, 17.06.2010: www.bbc.co.uk/news/10339543; dostęp: 21.10.2013; A. Bright: *Estonia accuses Russia of 'cyberattack'*. „The Christian Science Monitor" 17.05.2007: www.csmonitor.com/2007/0517/p99s01-duts.html; dostęp: 18.10.2013.

przyznał, iż to jego organizacja stoi za atakami komputerowymi na Estonię. Jego zdaniem nie wykorzystano w nich wcale komputerów rządowych, lecz urządzenia, które znajdowały się w Naddniestrzu, w Mołdawii. Na korzyść takiej interpretacji świadczył fakt, iż ok. 600 działaczy tej grupy blokowało równolegle estońską ambasadę w Moskwie oraz zakłóciło konferencję prasową estońskiej ambasador[39]. Podobne opinie, wątpiące w bezpośrednie zaangażowanie rosyjskich służb, wygłaszali również przedstawiciele amerykańskiej USCERT. Zdaniem Mike'a Witta cyberataki nie były na tyle zaawansowane technicznie, aby mogło to wskazywać na udział służb FR (za: Schackelford, 2009: 207—208).

Z drugiej strony pojawiły się głosy wskazujące na fakt, iż ocena tych incydentów nie powinna być tak jednoznaczna i kategoryczna. Jak wspomniano, o winie rządu rosyjskiego byli przekonani estońscy politycy i przedstawiciele tamtejszych służb specjalnych. Minister obrony Jaak Aaviksoo uznał na przykład, że te ataki były „masowe, świetne ukierunkowane i zorganizowane"[40]. Zarówno on, jak i inni przedstawiciele władz twierdzili, iż analiza adresów IP komputerów, z których przeprowadzono ataki, jasno świadczyła o odpowiedzialności Kremla. Zdaniem Tallina na winę Rosjan miał wskazywać również fakt, że Federacja odmówiła jakiejkolwiek współpracy w celu ukarania sprawców znajdujących się na jej terytorium. Mimo zapisów umowy o dwustronnej pomocy prawnej (*Mutual Legal Assistance Treaty* — MLAT) między oboma krajami prokuratura rosyjska odmówiła wsparcia śledztwa w tej sprawie (za: Schackelford, 2009: 208; szerzej: Barletta, 2010: 11—12). Minister sprawiedliwości Estonii Rain Lang stwierdził wręcz, iż w Moskwie przestano odbierać jego telefony. Między innymi na tej podstawie część analityków wskazywała, że cyberataki były zbyt dobrze zorganizowane i zaawansowane, aby mogli za nimi stać zwykli haktywiści i *script kiddies*. Konsultant rządu Estonii ds. IT Linnar Vik zauważył, iż chronologicznie ostatnie incydenty obejmowały środki, „których nie da się kupić na czarnym rynku", sugerując tym samym udział służb specjalnych[41]. Mógł o tym świadczyć także fakt zauważony przez Joshuę Davisa (2007) z magazynu „Wired". Przypomniał on bowiem, iż kilka tygodni wcześniej Kreml został oskarżony o wykorzystanie sieci *botnet* do blokowania witryn internetowych rosyjskich grup opozycyjnych, którym przewodził Garri Kasparow. Na zlecenie „Wired" firma Arbor Networks porównała obie operacje DDoS. Okazało się wówczas, że część sieci *botnet* wykorzystanych przeciwko ruchowi

[39] Moćkun, 2009, s. 4; *Russia: Monument Dispute with Estonia Gets Dirty*. Radio Free Europe, 04.05.2007: www.rferl.org/content/article/1076297.html; dostęp: 21.10.2013.

[40] R. Koman: *Estonia reeling from massive cyberattack from Russia*. ZDNet, 18.05.2007: www.zdnet.com/blog/government/estonia-reeling-from-massive-cyberattack-from-russia/3161; dostęp: 21.10.2013.

[41] P. Finn: *Cyber Assaults on Estonia Typify a New Battle Tactic*. „The Washington Post", 19.05.2007: www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html; dostęp: 21.10.2013.

Kasparowa zostało później użytych do ataków na rząd w Tallinie. Na tej podstawie jeden z opozycyjnych przywódców rosyjskich Denis Bilunow winą obarczył jeden z departamentów działających w ramach Federalnej Służby Bezpieczeństwa. Interesujące stanowisko zajął również Stephen Herzog (2011: 53) na łamach „Journal of Strategic Security". Według niego

> mając na uwadze zaawansowane rosyjskie zdolności prowadzenia cyberwojny oraz znaczenie ataków na Estonię, uzasadnione jest pytanie, czy były one przeprowadzone przez autonomiczne sieci rosyjskojęzycznych hakerów, czy też dokonał ich lub sponsorował je Kreml? Mimo że eksperci Unii Europejskiej i NATO nie byli w stanie znaleźć dowodów rosyjskiego udziału […], to bez wątpienia zorganizowanie uderzeń DDoS leżałoby w interesach Moskwy.

Na tym tle warto więc odwołać się do celów badawczych postawionych we wstępie, zadając kilka fundamentalnych pytań. Po pierwsze: jak można sklasyfikować cyberataki na Estonię zgodnie z typologią przedstawioną w poprzednim rozdziale? Innymi słowy: kim byli sprawcy oraz do jakich środków się odwoływali? Po drugie: jakie interesy i cele przyświecały tej kampanii z perspektywy teorii polityki zagranicznej? Po trzecie: jakie były reperkusje tych ataków, zarówno w wymiarze stosunków bilateralnych obu państw, ich polityk zagranicznych, jak i szerszej debaty nad wyzwaniami dla bezpieczeństwa międzynarodowego?

Trudno jednoznacznie ocenić, kto był bezpośrednio odpowiedzialny za organizację i przeprowadzenie tych cyberataków. Być może, jak sugerował Andrew W. Krepinevich, incydenty te były swoistym testem „cyberbroni" i ich użyteczności w warunkach kryzysu politycznego (Krepinevich, 2012: 24; Rosenfield, 2009: 83). Nie można jednak od razu odrzucić tezy wskazującej na głównie spontaniczny charakter tej kampanii. Przytoczone wyżej argumenty nie dają jednoznacznej odpowiedzi w tym zakresie. W pierwszym przypadku zastosowanie kategorii „pierwszej cyberwojny" byłoby uzasadnione, zgodnie bowiem z paremią prawniczą *is fecit, cui prodest* największą korzyść z ataków odniósł właśnie Kreml. W drugim należałoby uznać je za przejaw haktywizmu patriotycznego, wynikającego z napięć na linii Tallin — Moskwa. Bez względu na brak jednoznacznych dowodów najprawdopodobniej incydenty w Estonii stanowiły hybrydę złożoną z obu tych form zagrożeń teleinformatycznych, uznanie ich za pełnoprawną cyberwojnę byłoby zatem pewnym nadużyciem[42]. Z jednej strony jasne jest, że w atakach brali udział rosyjscy haktywiści, *script kiddies*, internetowi wandale oraz osoby przypadkowe, niezwiązane bezpośrednio z tym środowiskiem. Ich główną motywacją była chęć ukarania Estończyków nie tylko za usunięcie Brązowego Żołnierza, lecz także za wieloletnią, ich zdaniem, dyskryminację mniejszości oraz regularne napięcia polityczne. Protesty społeczne

[42] Stąd też ujęcie terminu *cyberwojna* w cudzysłów w tytule podrozdziału.

na tym tle były wszak widoczne i w wymiarze offline, dlatego pisanie o swoistych „zamieszkach" w cyberprzestrzeni nie było do końca nietrafione. Z drugiej jednak strony wątpliwości budzi fakt, iż wiele niezwiązanych ze sobą w żaden sposób grup było w stanie koordynować przez około trzy tygodnie masowe ataki komputerowe, które nie tylko paraliżowały strony internetowe, ale także naruszyły wybrane elementy infrastruktury krytycznej. Stopień ich organizacji, starannie dobrane cele, a także wykorzystane środki, w tym przede wszystkim liczące dziesiątki tysięcy komputerów sieci *botnet*, pozwalają wątpić w zupełny brak udziału rosyjskich służb specjalnych. Niekoniecznie musiał on oznaczać bezpośrednie zaangażowanie w cyberataki, mógł bowiem dotyczyć np. inspirowania związanych z Kremlem grup haktywistów patriotycznych, dostarczenia niezbędnych środków finansowych czy *know-how*.

Za taką interpretacją tych wydarzeń świadczą trzy sprawy. Po pierwsze, jak wspomniano, podobne instrumenty wykorzystano wcześniej przeciwko grupom opozycyjnym, wrogim wobec władzy Władimira Putina. Po drugie w kolejnych latach doszło do innych zmasowanych ataków teleinformatycznych, m.in. przeciwko Gruzji czy Ukrainie[43], których źródłem była Rosja. Działania w sieci przeciwko Estonii wpisywały się zatem pewną szerszą kampanią cyberataków wobec krajów obszaru poradzieckiego, z której korzyści czerpała wyłącznie Moskwa. Po trzecie wreszcie: nawet jeśli administracja państwowa bezpośrednio nie brała udziału w tych incydentach, to inspirowała je w wymiarze politycznym. Krytyczne wobec Estonii wypowiedzi Władimira Putina, Ministerstwa Spraw Zagranicznych FR oraz deputowanych Dumy jasno na to wskazywały. Odwołując się do wcześniejszych rozważań, można tu nawet mówić o zaistnieniu odpowiedzialności pośredniej Kremla wynikającej z tolerowania, zachęcania bądź nieukarania sprawców bezprawnych działań przeciwko innemu państwu (Bierzanek, Symonides, 2002: 154). Nie dość, że wypowiedzi decydentów polityki zagranicznej mogły być uznane za zachęcanie do cyberataków, to nie podjęto żadnych działań prewencyjnych w oparciu o umowę o pomocy prawnej, spełniało to więc przesłanki wynikające z norm prawa międzynarodowego, tym samym sugerowało przychylność administracji państwowej wobec sprawców. Na fakt ten zwrócili uwagę m.in. Richard A. Clarke i Robert K. Knake (2010: 15), którzy stwierdzili, że nawet jeśli za incydentami rzeczywiście stali „patriotyczni Rosjanie", to nie było sensownej odpowiedzi na pytanie, dlaczego Kreml oraz służby nie uczyniły nic, aby zapobiec aktom ewidentnej przestępczości komputerowej.

Mając to na uwadze, warto się zastanowić, jakie interesy i cele przyświecały cyberatakom przeciwko Estonii. W sensie praktycznym działania te wpisywały się w omówione wyżej założenia polityki zagranicznej Rosji wobec strefy

[43] Zob. D. Lee: *Russia and Ukraine in cyber 'stand-off'*, BBC News, 05.03.2014: www.bbc.com/news/technology-26447200; dostęp: 12.04.2014.

poradzieckiej. Incydenty teleinformatyczne były przede wszystkim kompromitacją państwa estońskiego. Udowodniły, że mimo wdrożonych zaawansowanych rozwiązań technologicznych nie było ono w stanie zabezpieczyć nie tylko sektora prywatnego czy serwerów administracji rządowej, lecz nawet elementów infrastruktury krytycznej. Tym samym znaleziono skuteczny środek przekreślający wizerunek Estonii jako modelowego przykładu transformacji w strefie poradzieckiej. Było to tym wyraźniejsze, iż wydarzenia te zostały dostrzeżone przez cały świat, a Estonia odegrała w nich rolę bezbronnej ofiary. Po drugie był to widowiskowy sposób wsparcia mniejszości rosyjskiej mieszkającej w tym kraju. Wcześniej działania podejmowane przez Kreml obejmowały głównie aktywność organizacji pozarządowych oraz naciski medialne, które nie wywierały jednak pożądanego wpływu na rząd w Tallinie. Dyskryminacyjna zdaniem Moskwy polityka Estonii nie uległa przez to zmianie, dlatego odwołanie się do bardziej inwazyjnych instrumentów mogło być próbą spektakularnego rewanżu. Po trzecie treści zamieszczane przez rosyjskich haktywistów m.in. na stronach internetowych rządu Ansipa świadczyły o oczywistym kontekście historycznym tych cyberataków. Wydaje się, iż działania te miały zagłuszyć i zdyskredytować estońską wykładnię wydarzeń z okresu drugiej wojny światowej, a tym samym były korzystne dla rosyjskiej polityki historycznej. Po czwarte wreszcie, jak sugerował Andrew W. Krepinevich, mogła to być rzeczywiście próba szerszego zastosowania tych unikalnych środków polityki zagranicznej w warunkach kryzysu w stosunkach bilateralnych. Federacja Rosyjska mogła w tej sytuacji chcieć sprawdzić swoje możliwości w tym zakresie. I to w dużej mierze się udało, ponieważ mimo porażki w sprawie monumentu Moskwa propagandowo wyszła z niego zwycięsko, udowodniono bowiem rządowi w Tallinie, iż można mu bez większego wysiłku zaszkodzić, nie ponosząc przy tym żadnego ryzyka. Reakcja władz Estonii, jej sojuszników oraz międzynarodowej opinii publicznej dawały ciekawy materiał poglądowy, który mógł być wykorzystany w kolejnych działaniach tego typu w przyszłości.

Odnosząc te rozważania do klasyfikacji celów polityki zagranicznej państwa zaproponowanej przez Ryszarda Zięb (2005a: 48—49), można wyciągnąć dwa wnioski. Przede wszystkim Federacja Rosyjska działała na rzecz wzrostu swojej siły. Skutecznie doprowadzając do kompromitacji państwa estońskiego, jego służb i administracji rządowej, stworzono sobie dogodne warunki do wywierania wpływu w strefie poradzieckiej. Wydaje się ponadto, iż cyberataki na Estonię należałoby uznać za działania na rzecz wzmocnienia pozycji i prestiżu państwa w stosunkach międzynarodowych, udowodniły one bowiem, że Federacja posiada wyjątkowy w swojej istocie potencjał w tej dziedzinie, choć akurat w tym przypadku nie został on w pełni ujawniony. Cyberataki przeciwko Estonii wzmocniły ponadto pozycję mniejszości rosyjskiej na obszarze poradzieckim, państwa tego regionu zdały sobie bowiem sprawę z możliwych konsekwencji w wypadku podobnych zajść w przyszłości.

Na koniec należy podkreślić, że incydenty te nie doprowadziły do nieodwracalnych zniszczeń bądź ogromnych strat finansowych, stały się jednak wyraźnym sygnałem tego, że przestrzeń teleinformatyczna może być sferą szkodliwej aktywności innych uczestników stosunków międzynarodowych. Wywołały zarazem burzliwą dyskusję poświęconą znaczeniu cyberprzestrzeni dla bezpieczeństwa państw. Z jednej strony stanowiły one symboliczne potwierdzenie opinii części środowiska naukowego, które od dawna wskazywało na rosnące wyzwania w tej dziedzinie, z drugiej uświadomiły wagę tych problemów światowej opinii publicznej oraz elitom politycznym (Ashmore, 2009: 8). W ciekawy sposób ujął to przywoływany już Stephen Herzog (2011: 56), który pisał, iż światowa gospodarka przystosowała się do ery cyfrowej, a wydarzenia w Estonii udowodniły, iż narodowe polityki zagraniczne i bezpieczeństwa muszą przystosować się do nowych uwarunkowań związanych z działaniami w cyberprzestrzeni. Wypada się zgodzić z tymi słowami, gdyż rzeczywiście był to silny impuls na rzecz zmian, o czym świadczyły m.in. reformy przeprowadzone przez państwa członkowskie NATO w kolejnych latach.

4.2. Cyberataki w stosunkach litewsko-rosyjskich

Kolejnym interesującym przykładem rosnącego znaczenia cyberprzestrzeni w rywalizacji międzypaństwowej na obszarze poradzieckim jest *casus* Litwy, która od drugiej połowy pierwszej dekady XXI wieku stawała się wielokrotnie ofiarą zmasowanych cyberataków. W przeciwieństwie do Estonii wydarzenia te nie spotkały się z porównywalnym zainteresowaniem światowych mediów, tym bardziej warto więc prześledzić ich bieg i znaczenie.

Analizę owych incydentów należałoby rozpocząć od charakterystyki podstawowych uwarunkowań stosunków litewsko-rosyjskich, które w swojej istocie są bardzo podobne do relacji na linii Tallin — Moskwa. Przede wszystkim również i tutaj zasadnicze znaczenie dla kontaktów bilateralnych zachowały kwestie historyczne, w których stroną dominującą od XVII wieku była Rosja. Wraz z upadkiem I Rzeczpospolitej pod koniec wieku XVIII ziemie litewskie znalazły się pod panowaniem caratu. Litwa odzyskała niepodległość dopiero w 1918 roku. W okresie międzywojennym stosunki z Kremlem pozostały jednak bardzo napięte, tym bardziej, iż ideologia komunistyczna była uznawana za zagrożenie dla tożsamości odradzającej się narodowości litewskiej. Wybuch II wojny światowej zakończył się ponownym upadkiem państwa litewskiego, kiedy w 1940 roku wojska radzieckie weszły na jego terytorium i rozpoczęły proces sowietyzacji i rusyfikacji, przerwany na krótko przez III Rzeszę. Po wyzwoleniu kraju przez Armię Czerwoną Litwa została włączona do Związku

Radzieckiego. Wówczas rozpoczął się trwający do połowy lat 50. okres masowego terroru i zsyłek na Syberię. Doświadczenia te, wraz z głębokim podporządkowaniem Kremlowi podczas zimnej wojny, wywoływały później poważne napięcia w stosunkach dwustronnych. Dotyczyły one m.in. okupacji z 1940 roku czy stosowania represji wobec Litwinów w kolejnych latach (zob. Laurinavičius, 2006: 124—125). Jak pisali Alfonsas Eidintas, Afredas Bumblauskas, Antanas Kulakauskas i Mindaugas Tamošaitis (2013: 238): „rządy sowieckie na Litwie powojennej były brzemienne w skutki dla jej mieszkańców: w czasach stalinowskich doszło do likwidacji przez władze okupacyjne tysięcy ludzi oraz całych grup społecznych, a także ich tradycji kulturalnych i mienia". Na suwerenność Litwa wybiła się dopiero dzięki narastającemu procesowi rozkładu wewnętrznego Związku Radzieckiego. W wyniku organizacji grup opozycyjnych od 1988 roku, 11 marca 1990 roku ogłoszono deklarację niepodległości, która wywołała ostrą reakcję władz ZSRR: wprowadzenie m.in. blokady gospodarczej państwa. Na początku 1991 roku doszło wręcz do użycia Armii Czerwonej w Wilnie, w wyniku czego zginęło 13 osób, a 580 zostało rannych. Bez względu na te tragiczne wydarzenia państwo ostatecznie odzyskało niepodległość i zostało uznane przez społeczność międzynarodową (Ibidem, s. 273—291).

Na tym tle polityka rosyjska wobec Litwy wpisywała się w szersze ramy strategii wobec całego obszaru poradzieckiego, podobnie jak miało to miejsce w stosunkach z Estonią. Moskwa od początku była zainteresowana utrzymaniem politycznych wpływów w Wilnie, sprzeciwiała się członkostwu tego kraju w Sojuszu Północnoatlantyckim, ochraniała swoją mniejszość w tym kraju, liczącą ponad 6% całości populacji[44] oraz pragnęła podtrzymywać korzystną dla siebie interpretację wspólnej historii (Topolski, 2013: 139—159). Co prawda jeszcze na początku lat 90. Kreml krytycznie oceniał skutki aneksji z 1940 roku, jednak wykładnia ta zmieniła się na przełomie XX i XXI wieku (Eidintas, Bumblauskas, Kulakauskas, Tamošaitis, 2013: 294—295).

Ze strony litewskiej szczególne znaczenie miało kilka czynników. Po pierwsze, podobnie jak w przypadku Estonii, dla Wilna fundamentalną rolę odgrywały kwestie związane z dysproporcją potencjałów obu państw. Dla Rosji Litwa pozostawała w okresie pozimnowojennym partnerem drugorzędnym, tymczasem dla Wilna działania Moskwy miały zasadnicze znaczenie (Nekrašas, 2004). Sprzyjało temu sąsiedztwo ze zmilitaryzowanym Obwodem Kaliningradzkim oraz utrzymujące się po rozpadzie ZSRR współzależności ekonomiczne, zwłaszcza w sektorze energetycznym. Po drugie po 1991 roku zasadnicze znaczenie zyskały sprawy związane z interpretacją wspólnej historii. Jak wspomniano, dość szybko władze rosyjskie odeszły od krytycznego spojrzenia na działania ZSRR

[44] *Ethnicities in Lithuania: Introduction*. True Lithuania: www.truelithuania.com/topics/culture-of-lithuania/ethnicities-of-lithuania; dostęp: 18.11.2013.

w latach 40. i 50. XX wieku, co wywoływało naturalną krytykę ze strony Litwy. Po trzecie stosunki z Moskwą odgrywały istotną rolę w kontekście prozachodnich aspiracji Wilna. Z jednej strony sceptycyzm Kremla w tej sprawie utrudniał realizowanie litewskich ambicji, z drugiej jednak wycofanie wojsk rosyjskich w 1993 roku z pewnością ułatwiło zabiegi o członkostwo Litwy w Sojuszu Północnoatlantyckim. Po czwarte wreszcie istotnym aspektem relacji z Rosją pozostawały elementy współpracy i rywalizacji gospodarczej, zwłaszcza w dziedzinie energetyki (Karabeshkin, 2007: 65—83).

Relacje litewsko-rosyjskie po roku 1991 były jednak zdecydowanie spokojniejsze niż kontakty na linii Tallin—Moskwa. Mimo antyrosyjskich postaw znacznej części społeczeństwa litewskiego oraz poczucia zagrożenia ze strony Federacji oba kraje stale ze sobą kooperowały na arenie międzynarodowej, szczególnie w wymiarze gospodarczym. O generalnie dobrej atmosferze świadczył fakt, iż przez kilkanaście lat nie wystąpiły większe problemy dotyczące rosyjskiej mniejszości na Litwie. Co naturalne, pojawiały się w nich regularne napięcia, które nie przekształcały się jednak w poważniejsze kryzysy polityczne. Dotyczyły one kilku spraw. Po pierwsze kontrowersje rodziła sprawa tranzytu przez terytorium Litwy osób, oddziałów wojskowych, towarów i surowców energetycznych z Obwodu Kaliningradzkiego. Kwestie te stały się szczególnie ważne w przeddzień akcesji Wilna do Unii Europejskiej, kiedy dotychczasowe mechanizmy musiały zostać dostosowane do reżimu układu z Schengen. Po drugie kontrowersje w wymiarze wewnętrznym wywoływały regularne próby przejęcia krajowego przemysłu energetycznego przez rosyjski kapitał. Po trzecie, szczególnie na początku lat 90. XX wieku, Litwa uznawała rosyjską obecność wojskową za spore zagrożenie, dlatego m.in. pojawił się pomysł powrotu do sojuszu z Łotwą i Estonią pod nazwą Rady Bałtyckiej. Po czwarte wreszcie, jak wspomniano, w okresie pozimnowojennym oba państwa dzieliła interpretacja wspólnej historii okresu Związku Radzieckiego (Miniotaitė, 2007: 177—193; Karabeshkin, 2007).

Do znacznego pogorszenia stosunków dwustronnych doszło dopiero w drugiej połowie pierwszej dekady XXI wieku. W 2006 roku Rosjanie odcięli dostawy ropy naftowej na Litwę rurociągiem „Przyjaźń", motywując to pracami konserwacyjnymi. Komentatorzy uznali jednak tę decyzję za zemstę za zwycięstwo PKN Orlen w rozgrywce o sprzedaż rafinerii w Możejkach[45]. W kwietniu 2008 roku Wilno zablokowało natomiast negocjacje Unii Europejskiej z Rosją w sprawie nowego układu o partnerstwie i współpracy. Motywując swoje stanowisko, wezwało UE do zaangażowania się w sprawy istotne z punktu widzenia interesów narodowych Litwy. Wymieniono tu m.in. wznowienie dostaw ropy naftowej do rafinerii w Możejkach, podjęcie rozmów na temat zamrożonych konfliktów w Mołdawii i Gruzji, współpracę z Rosją w sprawach karnych przed europej-

[45] D. Malinowski, A. Kublik: *Umowa zawarta. Orlen kupił Możejki*. Gazeta.pl, 26.05.2006: http://wiadomosci.gazeta.pl/wiadomosci/1,114873,3374478.html; dostęp: 18.11.2013.

skimi sądami czy wsparcie poszukiwań zaginionych w tym państwie Litwinów. Wilno domagało się ponadto nie tylko rekompensat dla osób zesłanych do gułagów po II wojnie światowej, lecz także postawienia przed sądem osób odpowiedzialnych za śmierć swoich obywateli w 1991 roku. W obu przypadkach Rosja nie wyrażała chęci współpracy[46]. Ostatnim elementem, który przyczynił się do kryzysu politycznego, była decyzja parlamentu litewskiego o zakazie prezentowania symboli komunistycznych, które zrównano z symbolami nazistowskimi. Karalne stało się m.in. demonstrowanie radzieckiej flagi, czerwonej gwiazdy, sierpa i młota oraz hymnu Związku Radzieckiego. Wpisało się to w podobne działania, które podjęła nieco wcześniej Estonia. Wywołało to oczywiście nerwowe reakcje Rosjan, którzy ten ruch określali mianem „bluźnierstwa", oskarżając państwa bałtyckie o próby „pisania historii na nowo". Zgodnie z wykładnią Kremla kraje te zostały wyzwolone spod okupacji nazistów, przez co mówienie o zbrodniach Armii Czerwonej było nadużyciem[47].

Tak więc podobnie jak w przypadku Estonii kryzys polityczny na linii Wilno — Moskwa pojawił się właśnie na tle odmiennych interpretacji historii. W tym kontekście po raz kolejny duże znaczenie odegrała przestrzeń teleinformatyczna[48], ponieważ symboliczną reakcją na uchwalone przez Litwinów nowe prawo stały się masowe cyberataki, które nastąpiły dwa tygodnie później, na przełomie czerwca i lipca 2008 roku. W ciągu jednego weekendu zaatakowano ok. 300 stron internetowych tego kraju, w tym zarówno witryny należące do rządu, jak i sektora prywatnego. Tym razem dominowały głównie metody *web defacement*, a nie DDoS. Chcąc ukarać rząd za wprowadzenie tego kontrowersyjnego dla Rosjan prawa, zaczęto zastępować znajdujące się na stronach internetowych materiały symbolami komunistycznymi bądź hasłami antylitewskimi[49]. Tak udana akcja

[46] *UE: Litwa blokuje negocjacje z Rosją*. Wprost.pl, 13.05.2008: www.wprost.pl/ar/129681/UE-Litwa-blokuje-negocjacje-z-Rosja; dostęp: 18.11.2013; *Pro-Russian cyber-attack hits Lithuania: regulator*. Agence France Presse, 30.06.2008: http://www.google.com/hostednews/afp/article/ALeqM5hAcDZhvTbYvScNQ55FI0FVRw2BFw?hl=en; dostęp: 18.11.2013.

[47] *Lithuania equates Soviet symbols with Nazism*. Pravda.ru, 17.06.2008: http://english.pravda.ru/world/ussr/17-06-2008/105526-soviet_symbols-0; dostęp: 18.11.2013; *Lithuanian ban on Soviet symbols*. BBC News, 17.06.2008: http://news.bbc.co.uk/2/hi/europe/7459976.stm; dostęp: 18.11.2013.

[48] Warto jednak zauważyć, iż Litwa w odróżnieniu od Estonii była nieco mniej zaawansowana pod względem wykorzystania technologii teleinformatycznych. Co prawda w *ICT Development Index* z 2008 roku zajmowała ona 35. miejsce, to jednak zakres integracji ICT w funkcjonowanie administracji państwowej czy sektora prywatnego był zdecydowanie mniejszy niż w przypadku Tallina. Zob. *Lithuania Country Report*, 2011; *Measuring the Information Society*, 2011, s. 13.

[49] Zob. E. Tikk, 2011, nr 3 (53); S. Rhodin: *Hackers Tag Lithuanian Web Sites With Soviet Symbols*. „The New York Times" 01.07.2008: www.nytimes.com/2008/07/01/world/europe/01baltic.html?_r=2&scp=3&sq=lithuania&st=nyt&oref=slogin&; dostęp: 18.11.2013; Shetty, Kearns, Lunn, 2012, s. 9.

była możliwa dzięki złamaniu zabezpieczeń tylko jednego serwera należącego do litewskiego dostawcy usług internetowych (ISP) Hostex. Warto dodać, iż tym razem użyto zainfekowanych komputerów znajdujących się w Europie Zachodniej, w tym głównie we Francji[50]. Analizę tych incydentów teleinformatycznych stosunkowo szybko przeprowadziła korporacja Idefense zajmująca się bezpieczeństwem informacyjnym. Według jej ekspertów sprawcami cyberataków okazali się rosyjscy haktywiści (patriotyczni), którzy skupili się wokół strony www.hack-wars.ru. Jak sami twierdzili, ich celem były wspólne ćwiczenia i koordynacja, tak aby stworzyć zorganizowaną siłę zdolną do działań w cyberprzestrzeni w imię obrony interesów Rosji. Swoje zamierzenia zawarli w manifeście rozsyłanym w litewskim internecie za pomocą spamu pt. *Hackers United against External Threats to Russia*. Zapowiedziano w nim szerszą kampanię cyberataków, do której celów zaliczono Ukrainę, inne państwa bałtyckie, a także kraje członkowskie NATO ze względu na popierany przez nie proces poszerzania tej organizacji na wschód[51]. Podobne stanowisko zajął szef litewskiego LITNET (Academic and Research Network) CERT Marius Urkis, który zauważył w lipcu 2008 roku, iż za atakami mogli stać zwykli Rosjanie, oburzeni podjętą przez Wilno decyzją. Przy czym należy pamiętać, iż litewski rząd, w przeciwieństwie do estońskiego, nie oskarżył Kremla o udział w tych incydentach[52].

W trzy tygodnie później doszło do drugiej fali cyberataków przeciwko Litwie. Tym razem użyto metod DDoS przeciwko stronie internetowej państwowego urzędu skarbowego. Sprawcy korzystali z komputerów znajdujących się w Rumunii, ich źródłem była jednak prawdopodobnie znowu Rosja, choć nie zdobyto na to nigdy jednoznacznych dowodów[53]. Jak zauważył szef inspektoratu podatkowego Gediminas Vysniauskis, możliwe, iż były one zaplanowane już wcześniej, co świadczyłoby o kontynuacji kampanii z przełomu czerwca i lipca. Tym razem udało się zapobiec poważniejszym szkodom. Jedynym rezultatem tych incydentów było zakłócenie możliwości składania oświadczeń podatkowych online[54].

---

[50] E. Tikk: *Frameworks for International Cyber Security.* Cooperative Cyber Defense Centre of Excellence: https://www.nsm.stat.no/upload/konferanser%2009/05_framework%20of%20cyber%20incident_tikk.pdf; dostęp: 13.12.2013.

[51] B. Krebs: *Lithuania Weathers Cyber Attack, Braces for Round 2*. „The Washington Post" 03.07.2008: http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html; dostęp: 18.11.2013; Denning, 2011: 181.

[52] J. Kirk: *Lithuania: Attacks focused on hosting company.* „Computer World" 04.07.2008: www.computerworld.com/s/article/9106878/Lithuania_Attacks_focused_on_hosting_company?taxonomyId=17&intsrc=kc_top&taxonomyName=security; dostep: 13.12.2013.

[53] *Lithuania cyber attacks: Round two.* „The Baltic Times" 22.07.2008: www.baltictimes.com/news/articles/20897; dostęp: 18.11.2013.

[54] *Lithuanian tax office website hit by cyber attack*, Reuters, 21.07.2013: www.reuters.com/article/2008/07/21/lithuania-web-attacks-idUSMAR14153920080721; dostęp: 13.12.2013.

Doświadczenia z 2008 roku nie doprowadziły, jak można było oczekiwać, do większego zainteresowania się tą problematyką ze strony władz w Wilnie[55]. Jak zauważyła Vaiva Sapetkaitė, co prawda przyjęto plan rozwoju polityki bezpieczeństwa informacyjnego na lata 2011—2019, jednak ze względu na kryzys gospodarczy nie przeznaczono na jego wdrażanie niezbędnych środków finansowych[56]. W efekcie zdolność litewskiego zespołu reagowania na incydenty komputerowe CERT-LT była mocno ograniczona. Między innymi świadczył o tym fakt, iż ze względu na braki kadrowe dopiero w 2013 roku zaczął on działać 24 godziny na dobę, 7 dni w tygodniu[57]. Zaniedbania w tej dziedzinie według wielu sygnałów, które docierały do mediów w ostatnich latach, były wielokrotnie wykorzystywane przez rosyjskich cyberprzestępców i haktywistów patriotycznych. Zwróciło na to uwagę litewskie Ministerstwo Obrony, jeden z pracujących tam ekspertów Algimantas Melaikis w czerwcu 2013 roku zauważył bowiem zjawisko narastającego cyberszpiegostwa, wiążącego się głównie ze sprowadzanym ze wschodu sprzętem komputerowym oraz programami użytkowymi. Jego zdaniem tego typu produkty posiadały coraz częściej specjalnie przygotowane luki w zabezpieczeniach, które umożliwiały zdalny i nieautoryzowany dostęp do litewskich komputerów i sieci. Służyły do tego m.in. trojany zaprojektowane w taki sposób, aby zbierać informacje o zainfekowanych systemach i znajdujących się w nich danych, pozostając jednocześnie w ukryciu[58].

Nie może więc dziwić fakt, iż w maju 2013 roku po raz kolejny cyberataki odegrały pewną rolę w stosunkach litewsko-rosyjskich. Incydenty w przestrzeni teleinformatycznej tym razem zostały zainspirowane nie problemami historycznymi, lecz, co zaskakujące, konkursem Eurowizji. W jego trakcie popularny litewski portal DELFI ujawnił informacje, według których Rosjanie oferowali Litwinom pieniądze w zamian za głosy oddawane na zespół reprezentujący Federację. Niedługo później jego redaktorzy otrzymali napisaną po rosyjsku wiadomość e-mail, w której szantażysta zagroził zablokowaniem strony, jeśli w ciągu godziny nie usunięto by informacji godzących w dobre imię Rosji oraz jej reprezentantki Diny Garipowej. DELFI odmówiło, co w rezultacie doprowadziło do zapowiadanego

[55] Dopiero w czerwcu 2012 roku Sejm litewski przyjął Narodową Strategię Bezpieczeństwa. Wśród głównych interesów bezpieczeństwa Litwy wymieniono tam m.in. cyberbezpieczeństwo, zapowiedziano wsparcie natowskich inicjatyw w zakresie bezpieczeństwa teleinformatycznego oraz wykształcenie wojskowych zdolności odpierania cyberataków. Zob. *Resolution Amending the Seimas*, 2012.

[56] V. Sapetkaitė: *Cybernetic (in)security: situation in the Baltic States*. Geopolitika.lt, 06.08.2012: www.geopolitika.lt/?artc=5541; dostęp: 13.12.2013.

[57] *Lithuanian national Computer Emergency Response Team would work for 24 hours a day*. The Baltic Course, 11.06.2013: www.baltic-course.com/eng/Technology/?doc=76106; dostęp: 13.12.2013.

[58] *Military intelligence officer claims that equipment from the East contains spyware*. „The Lithuania Tribune" 06.06.2013: http://www.lithuaniatribune.com/40753/military-intelligence-officer-claims-that-equipment-from-the-east-contains-spyware-201340753; dostęp: 13.12.2013.

cyberataku. Zastosowano tutaj metodę DDoS w oparciu o stosunkowo dużą sieć *botnet*, składającą się z komputerów znajdujących się m.in. w Turcji, Rosji, Brazylii oraz Japonii[59]. Jak ocenił Pranas Slušnys, trwający ponad tydzień atak osiągnął rekordową skalę ze względu na swą długość, jak i potencjał wykorzystanych środków[60]. Świadczył o tym fakt, iż przepustowość ataku wyniosła aż 6 Gb/s[61]. Poza DELFI blokada objęła także inne popularne litewskie media internetowe, w tym np. portale 15min.lt, irytas.lt, alfa.lt, irt.lt, diena.lt oraz bernardinai.lt.

Wydarzenia te zwróciły naturalnie uwagę władz państwowych oraz międzynarodowej opinii publicznej, zaczęto bowiem zadawać pytanie, czy tak z pozoru błaha sprawa rzeczywiście mogła wiązać się z tak poważnymi konsekwencjami. Dyskusja na ten temat rozpoczęła się już pod koniec maja 2013 roku, co wiązało się m.in. z oświadczeniem Litewskiego Stowarzyszenia Mediów Internetowych (Lithuanian Internet Media Association), w którym wyrażono „głębokie zaniepokojenie bezpieczeństwem Internetu na Litwie", wzywając instytucje państwowe do podjęcia wzmożonych wysiłków w tej dziedzinie. Zauważono przy tym związek między istotnymi incydentami teleinformatycznymi a ważnymi wydarzeniami politycznymi i kulturalnymi[62]. Spotkało się to w końcu z reakcją litewskiego rządu, który opublikował raport wskazujący na agresywne działania rosyjskich i białoruskich służb specjalnych w cyberprzestrzeni[63]. Stanowisko to podzielali również rodzimi eksperci i komentatorzy, przekonani o politycznym podłożu incydentów komputerowych. Przykładowo według Edvardasa Pociusa wiązały się one z dwoma wydarzeniami. Jednym było zakończenie tydzień przed atakiem na DELFI konferencji Baltic Cyber Security Forum, która została zorganizowana w Wilnie, drugim było natomiast rozpoczynające się 1 lipca 2013 roku przewodnictwo Litwy w Unii Europejskiej[64]. Z taką interpretacją zgodzili się także przedstawiciele elit politycznych. Artūras Paulauskas, przewodniczący

[59] *DELFI news portal was threatened and later attacked*. „The Lithuania Tribune" 22.05.2013: http://lithuaniatribune.com/38842/delfi-news-portal-was-threatened-and-later-attacked-201338842; dostęp: 13.12.2013.

[60] *IT specialists say that cyber attack on news portal DELFI is 'record'*. „The Lithuania Tribune" 28.05.2013: www.lithuaniatribune.com/39514/it-specialists-say-that-cyber-attack-on-news-portal-delfi-is-record-201339514; dostęp: 13.12.2013.

[61] C. Pierdet: *Cyber-attack on a Lithuanian news portal*. Economie-numerique.net, 20.07.2013: http://blog.economie-numerique.net/2013/07/20/cyber-attack-on-a-lithuanian-news-portal; dostęp: 13.12.2013.

[62] *More state support needed to curb cyber attacks in Lithuania*. „The Lithuanian Tribune" 29.05.2013: www.lithuaniatribune.com/39640/more-state-support-needed-to-curb-cyber-attacks-in-lithuania-201339640; dostęp: 13.12.2013.

[63] *Rasa Junkevičienė on cyber attacks: Ministry of the Interior should take the blame*. „The Lithuania Tribune" 12.06.2013: www.lithuaniatribune.com/41366/rasa-jukneviciene-on-cyber-attacks-ministry-of-the-interior-should-take-the-blame-201341366; dostęp: 13.12.2013.

[64] E. Pocius: *Opinion: Cyber attack on Delfi — not so bad after all?* „The Lithuania Tribune" 24.05.2013: www.lithuaniatribune.com/39085/opinion-cyber-attack-on-delfi-not-so-bad-after-all-201339085; dostęp: 13.12.2013.

Narodowego Komitetu Bezpieczeństwa i Obrony, stwierdził, że wydarzenia te były ważnym sygnałem przed objęciem przez Litwę przewodnictwa w UE, a atak na media krajowe uznał za problem zawierający się w kategorii bezpieczeństwa narodowego[65]. Natomiast prezydent Daila Grybauskaitė na początku czerwca 2013 roku wezwała agencje rządowe do dołożenia większych starań, aby zapewnić bezpieczeństwo teleinformatyczne państwa. Przyznała przy tym, iż dotychczasowe wysiłki w tej dziedzinie były niewystarczające[66]. Warto dodać, iż litewskie władze obawiały się powtórzenia scenariusza hiszpańskiego: w trakcie prezydencji Madrytu w Unii Europejskiej jej oficjalna strona internetowa została zablokowana. Podobny incydent oznaczałby więc dla Wilna daleko idącą kompromitację w całej Europie[67].

Mając na uwadze powyższe rozważania, można zwrócić uwagę na kilka istotnych spraw. Przede wszystkim należy stwierdzić, iż cyberataki przeciwko Litwie nigdy nie osiągnęły takiej skali, jak w przypadku Estonii. W 2008 roku odwołano się raptem do najbardziej standardowych metod, takich jak *web defacement*. Ataki metodą DDoS okazały się z kolei nieliczne i mało skuteczne. Co prawda doprowadziły one do pewnych zakłóceń, jednak tylko w ograniczonym zakresie. Nieco groźniejsze były z pewnością incydenty z 2013 roku. Mimo że ich skala była o wiele większa niż 5 lat wcześniej, to głównym ich celem były media elektroniczne. Nie zagroziły one natomiast elementom infrastruktury krytycznej państwa oraz funkcjonowaniu administracji publicznej. Taką interpretację wydarzeń potwierdził zresztą minister spraw wewnętrznych Litwy Aflonsas Barakauskas, który w lipcu 2013 roku na nieformalnym spotkaniu UE w Wilnie stwierdził, iż kraj ten nie napotkał jeszcze poważnych wyzwań w sferze cyberbezpieczeństwa. Jednocześnie podkreślił jednak, że członkowie Unii Europejskiej powinni pogłębiać swoją współpracę w tej dziedzinie[68]. Po drugie powstaje pytanie, kto był w takim razie odpowiedzialny za te cyberataki. W pierwszym przypadku winę ponosili rosyjscy haktywiści patriotyczni, nie pojawiły się bowiem żadne przesłanki, które mogłyby wskazywać na udział służb Federacji. Najdobitniej świadczyły o tym zresztą badania przeprowadzone przez Idefense oraz stanowisko LITNET CERT. Wbrew niektórym sugestiom również i w drugim przypadku trudno było oskarżać o bezpośredni udział rosyjskie agencje rządowe, zarówno

[65] *Paulauskas sees cyber attacks as important signal before EU presidency*. „The Lithuania Tribune" 29.05.2013: www.lithuaniatribune.com/39672/paulauskas-sees-cyber-attacks-as-important-signal-before-eu-presidency-201339672; dostęp: 13.12.2013.

[66] *President Grybauskaitė thinks that cyber security is taken primitively in Lithuania*. „The Lithuania Tribune" 04.06.2013: www.lithuaniatribune.com/40374/president-grybauskaite-thinks-that-cyber-security-is-taken-primitively-in-lithuania-201340374; dostęp: 13.12.2013.

[67] *Lithuanian parliament panel to look into cyber attack against online publication*. 15min.lt, 28.05.2013: www.15min.lt/en/article/in-lithuania/lithuanian-parliament-panel-to-look-into-cyber-attack-against-online-publication-525-339765; dostęp: 13.12.2013.

[68] *Interior min: so far Lithuania has not encountered real cyber attacks*. The Baltic Course, 19.07.2013: www.baltic-course.com/eng/Technology/?doc=77964; dostęp: 13.12.2013.

ze względu na zupełny brak dowodów, jak i na stosunkowo proste metody wykorzystywane przez sprawców. Cyberataki z lat 2008 i 2013 należałoby zatem sklasyfikować raczej jako przejaw haktywizmu patriotycznego, będącego częstym zjawiskiem w strefie poradzieckiej. Po trzecie wreszcie warto podkreślić, iż mimo braku dowodów na bezpośredni udział Kremla incydenty teleinformatyczne wywarły pewien ograniczony wpływ na pozycję międzynarodową Litwy, Rosji oraz stosunki dwustronne. W obu przypadkach ujawniły zasadniczą słabość zabezpieczeń komputerowych kolejnego państwa bałtyckiego. Stanowiły także symboliczną „karę" dla rządu, który zdecydował się wejść w otwarty spór historyczny z Moskwą. Tym samym osłabiono prestiż Litwy na arenie międzynarodowej, a także jej pozycję w stosunkach z Federacją Rosyjską. Równolegle w ograniczonym zakresie incydenty te poprawiły status Kremla na obszarze poradzieckim, ponieważ aktywność haktywistów patriotycznych ułatwiła realizację podstawowych założeń rosyjskiej polityki zagranicznej wobec państw bałtyckich, która przewidywała podkopanie ich rangi na arenie międzynarodowej. W oczach partnerów władze w Wilnie, które nie potrafiły zapobiec prostym cyberatakom, nie mogły się jawić jako poważny partner w Europie. Współgrało to również z działaniami na rzecz przekreślenia wizerunku Litwy, Łotwy czy Estonii jako wzorcowych przykładów transformacji ustrojowej w strefie poradzieckiej. Szczególną rolę odegrały tu wydarzenia z 2013 roku, które osłabiły prestiż Litwy przed ważnym dla niej momentem, jakim było przejęcie przewodnictwa w Unii Europejskiej. Kłopoty Wilna były jak najbardziej na rękę władzom w Moskwie i wpisywały się w inne podejmowane przez nią inicjatywy w wymiarze politycznym lub gospodarczym[69]. Na koniec warto zauważyć, iż zablokowanie najważniejszych mediów internetowych miało jeszcze dwojakie konsekwencje. Z jednej strony świadczyło to o zrozumieniu przez haktywistów patriotycznych, iż zakłócenie ich działalności może przynieść pewne korzyści polityczne zainteresowanym podmiotom. Z drugiej strony mogły one być interpretowane jako swoiste ostrzeżenie dla środowiska dziennikarskiego, aby nie publikować niekorzystnych dla Federacji Rosyjskiej materiałów. Reasumując, nie można więc mówić o odwołaniu się do cyberataków jako środka polityki zagranicznej, lecz o tolerowaniu bezprawnych, acz korzystnych dla Kremla działań.

[69] Można tu wspomnieć np. o dodatkowych kontrolach na granicy litewsko-rosyjskiej od sierpnia 2013 roku czy napięciach wokół cen gazu sprzedawanego przez Gazprom oraz stowarzyszenia Ukrainy z Unią Europejską. Zob. *Lithuania looks for alternatives to counter Russia's high gas price*. EurActiv, 03.07.2013: www.euractiv.com/energy/lithuanian-minister-gazprom-know-news-529127; dostęp: 13.04.2014; *EU calls on Russia to stop extra border checks from Lithuania*. Reuters, 17.09.2013: www.reuters.com/article/2013/09/17/us-lithuania-russia-idUSBRE98G0XY20130917; dostęp: 13.04.2014.

4.3. Wojna gruzińsko-rosyjska

Badając przejawy rywalizacji państw w cyberprzestrzeni na obszarze poradzieckim, nie można pominąć konfliktu zbrojnego, który miał miejsce na Kaukazie w sierpniu 2008 roku. Analizując ten *casus*, należałoby ponownie rozpocząć od charakterystyki uwarunkowań stosunków dwustronnych, tym razem między Gruzją a Federacją Rosyjską. Podobnie jak w przypadku Estonii czy Litwy w okresie pozimnowojennym jednym z głównych determinantów relacji gruzińsko-rosyjskich była wspólna historia, w której rolę dominującą odgrywała Moskwa. Świadczył o tym fakt, iż Tbilisi znajdowało się pod panowaniem rosyjskim od końca XVIII wieku aż do 1991 roku, z krótką przerwą po I wojnie światowej, sprzyjało to więc postrzeganiu Kremla przez Gruzinów jako naturalnego zagrożenia dla własnej państwowości[70].

Od momentu wybicia się Gruzji na niepodległość w wyniku rozpadu Związku Radzieckiego stosunki dwustronne były dość trudne i skomplikowane. Z jednej strony warto zauważyć, iż pierwszy gruziński prezydent Zwiad Gamsakhurdia został obalony na przełomie 1991 i 1992 roku przez posiadającego silne związki z Rosją Eduarda Szewardnadze[71]. Z drugiej na linii Tbilisi — Moskwa pojawiło się wówczas wiele poważnych nieporozumień, wynikających z odmiennych wizji relacji dwustronnych oraz kształtu Kaukazu w okresie pozimnowojennym. W konsekwencji doprowadziło to do sytuacji, w której zdecydowana większość gruzińskich elit politycznych właśnie w Federacji Rosyjskiej zaczęła widzieć główne zagrożenie dla integralności terytorialnej kraju. Taką optykę potwierdzało zresztą poparcie, jakiego Moskwa udzieliła walczącym o niezależność mniejszościom etnicznym na Kaukazie: Abchazom oraz Osetyjczykom[72].

Rosnące w latach 90. XX wieku napięcie w stosunkach dwustronnych doprowadziło do sytuacji, w której Gruzja zaczęła upatrywać swoich szans w nawiązaniu bliższych relacji z krajami zachodnimi. Szczególną rolę pełniły tu Stany Zjednoczone, które od pewnego czasu interesowały się przejęciem kontroli nad surowcami energetycznymi w rejonie Morza Kaspijskiego (Bryc, 2006: 88). Polityka gruzińska wpisała się więc w szersze spektrum rywalizacji

[70] *Georgia Background*. The World Factbook, Central Intelligence Agency: www.cia.gov/library/publications/the-world-factbook/geos/gg.html; dostęp: 16.12.2013.

[71] Zob. Bohlen, 1993; L.R. Urushadze: *Zviad Gamsakhurdia — the first President of Georgia*. Archive.org: http://archive.org/stream/ZviadGamsakhurdia-TheFirstPresidentOfGeorgia/ZviadGamsakhurdia_djvu.txt; dostęp: 16.12.2013.

[72] Szerzej na ten temat w: German, 2006: 6—7; G. Khutsishvili: *Intervention in Transcaucasus*, „Perspective" 1994, nr 3, Institute for the Study of Conflict, Ideology and Policy: www.bu.edu/iscip/vol4/Khutsishvili.html; dostęp: 16.12.2013; Grochmalski, 2003: 356; *Russia behind Georgia plot*. BBC News, 24.05.1999: http://news.bbc.co.uk/2/hi/europe/351760.stm; dostęp: 16.12.2013.

rosyjsko-amerykańskiej na tym obszarze. Jak zauważył Mohammad Soltanifar (2005), zjawisko to wynikało głównie z odmiennych celów polityki zagranicznej Rosji oraz Stanów Zjednoczonych. Federacja chciała w tym regionie przede wszystkim wzmocnić swoją wieloletnią dominację w wymiarze politycznym, gospodarczym oraz wojskowym, USA tymczasem zaczęły inwestować w tamtejszy sektor energetyczny oraz rozwinęły bliską współpracę militarną z częścią państw tego obszaru. Natomiast zdaniem Macieja Falkowskiego, „jednym z priorytetów polityki Kremla na Kaukazie jest niedopuszczenie do ingerencji innych państw w sprawy regionu”[73]. Chodziło tu m.in. właśnie o Gruzję, dla której współpraca z USA stanowiła możliwość zredukowania zagrożenia ze strony Rosji (szerzej: Kim, Eom, 2008: 85—106). Doprowadziło to do sytuacji, w której w 2002 roku kraj ten został objęty amerykańskim *Georgia Train and Equip Program*. Polegał on z jednej strony na przekazaniu środków finansowych na modernizację armii, z drugiej natomiast na rozmieszczeniu na jej terytorium amerykańskich sił specjalnych, które miały prowadzić szkolenia wybranych oddziałów[74].

Do zasadniczego przełomu w stosunkach gruzińsko-rosyjskich doszło jednak dopiero w wyniku „rewolucji róż”, która miała miejsce w listopadzie 2003 roku. W jej wyniku w styczniu 2004 roku władzę w Tbilisi objął wykształcony w Stanach Zjednoczonych prawnik Michaił Saakaszwili. Był to polityk, który sformułował odmienną od poprzednika wizję polityki zagranicznej Gruzji. Przede wszystkim warto zauważyć, iż była to koncepcja zdecydowanie prozachodnia, która obrała kurs jednoznacznie konfrontacyjny wobec Federacji Rosyjskiej. Warto tu przywołać opinię Nikolaia Silajeva oraz Tengiza Pkhaladze (2011: 12), którzy wyróżnili kilka podstawowych celów polityki zagranicznej Gruzji na początku XXI wieku: suwerenność oraz integralność terytorialną, osiągnięcie trwałego rozwoju gospodarczego oraz bezpieczeństwa energetycznego, rozwój demokracji, społeczeństwa obywatelskiego oraz ochronę praw człowieka, integrację ze strukturami europejskimi i euroatlantyckimi, zapewnienie geopolitycznego znaczenia euroazjatyckiego korytarza transportowego, a także kulturowego i gospodarczego znaczenia Kaukazu. Zdaniem badaczy główną przeszkodą dla realizacji powyższych założeń była w oczach Tbilisi właśnie Moskwa. Podstawowym celem Saakaszwilego, który był warunkiem osiągnięcia pozostałych priorytetów, było odzyskanie pełnej kontroli nad zbuntowanymi obszarami kraju. Świadczyły o tym wydarzenia z 2004 roku, kiedy Tbilisi zmusiło do ustąpienia prezydenta autonomicznej Adżarskiej Republiki Autonomicznej Asłana Abaszydze. Odzyskując kontrolę nad Adżarią, wykonano najprostszą część planu, ta

[73] Choć należy tu zauważyć, iż autor odnosił się bardziej do Kaukazu Północnego. Te same cele były jednak formułowane także w przypadku stosunków z krajami Kaukazu Południowego. Zob. Falkowski, 2004, s. 15.

[74] I.R. Areshidze: *Helping Georgia?* „Perspective” 2002, nr 4, Institute for the Study of Conflict, Ideology and Policy: http://www.bu.edu/iscip/vol12/areshidze.html; dostęp: 16.12.2013.

nie miała bowiem możliwości uzyskania wsparcia ze strony Kremla (German, 2006). Zdecydowanie trudniejsze było natomiast podporządkowanie Osetii Południowej oraz Abchazji. W tym celu Saakaszwili podjął wielotorowe działania. Po pierwsze zaczęto intensywnie przygotować siły zbrojne do konfrontacji ze zbuntowanymi republikami. Świadczyło o tym radykalne podniesienie wydatków na zbrojenia, do pułapu ok. 10% PKB. Pozwoliło to na znaczące zakupy sprzętu wojskowego, sprowadzanego m.in. ze Stanów Zjednoczonych, Ukrainy, Izraela oraz Polski. Zdecydowano ponadto o podniesieniu liczebności armii gruzińskiej do 37 000 żołnierzy, choć nie udało się go osiągnąć przed sierpniem 2008 roku[75]. Po drugie symbolicznym wyrazem zamiarów prezydenta Saakaszwilego było również zacieśnienie współpracy wojskowej z państwami Sojuszu Północnoatlantyckiego, w tym przede wszystkim z USA oraz Turcją. Przejawiała się ona przede wszystkim organizacją wspólnych ćwiczeń i manewrów[76]. Po trzecie usunięto wojska rosyjskie z terytorium Gruzji, nie licząc oczywiście sił pokojowych na obszarach poza kontrolą Tbilisi. Po czwarte podjęto szereg interesujących inicjatyw dyplomatycznych, których celem było gruzińskie członkostwo w strukturach Paktu Północnoatlantyckiego, co miało zabezpieczyć kraj przed ewentualną interwencją rosyjską. Postulaty te, jakkolwiek zyskały zrozumienie w Waszyngtonie oraz krajach Europy Środkowej, zostały odrzucone przez tradycyjnie prorosyjsko nastawione Niemcy oraz Francję. Wyrazem tego stały się decyzje szczytu NATO w Bukareszcie w kwietniu 2008 roku[77]. Podjęto także próbę polubownego porozumienia z Abchazją oraz Osetią Południową: w 2007 roku zaproponowano im odzyskanie autonomii na zasadach, na których funkcjonowała Adżaria, jednak zarówno Cchinwali, jak i Suchomi odrzuciły te propozycje (Lakomy, 2010a: 181).

Z perspektywy Tbilisi tego typu sytuacja stwarzała bardzo poważne zagrożenie, obie republiki w coraz większym stopniu wyrażały bowiem chęć przyłączenia się do Federacji Rosyjskiej, na co przychylnie spoglądały władze w Moskwie. Rodziło to więc realną groźbę naruszenia integralności terytorialnej Gruzji. O prawdopodobieństwie takiego scenariusza świadczył również fakt, iż już w 1991 roku aż 90% obywateli Osetii Południowej w referendum opowiedziało się za takim scenariuszem. Ponadto jej przywódca Eduard Kokoity

[75] T. Hypki: *Kaukaskie Kosowo*. Agencja Lotnicza Altair, 17.08.2008: www.altair.com.pl/news/view?news_id=1535; dostęp: 16.12.2013.

[76] N. Shachtman: *How Israel Trained and Equipped Georgia's Army*. „Wired" 19.08.2008: www.wired.com/dangerroom/2008/08/did-israel-trai; dostęp: 16.12.2013; A. Mikhailov: *Is Ukraine ashamed of its infamous military cooperation with Georgia?* Pravda.ru, 02.10.2012: http://english.pravda.ru/world/ussr/02-10-2012/122326-ukraine_georgia_military-0; dostęp: 16.12.2013; J. Kucera: *Georgia: Measuring Tbilisi's Security Ties to Washington*. Euroasianet.org, 06.02.2012: www.eurasianet.org/node/64963; dostęp: 16.12.2013.

[77] Gallis, 2008; *NATO Expansion Defeat: France and Germany Thwart Bush's Plans*. Spiegel Online, 03.04.2008: www.spiegel.de/international/world/nato-expansion-defeat-france-and-germany-thwart-bush-s-plans-a-545078.html; dostęp: 16.12.2013.

w 2004 roku stwierdził, że aż 95% populacji tego kraju przyjęło rosyjskie obywatelstwo (German, 2006: 6—8).

Na tym tle od 2006 roku zaczęło dochodzić do coraz poważniejszych napięć na linii Tbilisi — Moskwa. Wyrazem tego był skandal szpiegowski, w którego wyniku z Gruzji usunięto kilku rosyjskich wojskowych. Ponadto w lecie 2006 roku gruzińskie siły specjalne zajęły strategicznie położony Wąwóz Kodorski. Od tego momentu zaczęło dochodzić do regularnych walk z separatystami. Pogłębiający się kryzys w stosunkach dwustronnych osiągnął apogeum już dwa lata później, na co złożyło się kilka spraw. Pierwszą z nich było uznanie przez kraje zachodnie niepodległości Kosowa, co wywołało ostry sprzeciw dyplomacji rosyjskiej. Odnosząc się do tego wydarzenia, minister spraw zagranicznych Federacji Siergiej Ławrow stwierdził, iż będzie to precedens, który może zostać wykorzystany także na Kaukazie (Lakomy, 2010a: 181—182). Drugą kwestią były narastające zbrojenia po stronie gruzińskiej, czemu towarzyszyła pogłębiona współpraca wojskowa ze Stanami Zjednoczonymi. Symbolem tego były m.in. manewry *Immediate Response 2008*. Po drugiej strony granicy w tym samym czasie prowadzono ćwiczenia *Kaukaz 2008*[78]. Po trzecie przyczyniły się do tego coraz częstsze incydenty graniczne wskazujące na zbliżający się konflikt (Lakomy, 2010a: 182).

Widać więc wyraźnie, iż interesy i cele polityk zagranicznych obu państw w kontekście sytuacji w Abchazji oraz Osetii Południowej były diametralnie różne: Tbilisi dążyło do zapewnienia integralności terytorialnej kraju oraz zawiązania trwałego sojuszu z państwami zachodnimi, tymczasem dla Federacji Rosyjskiej działania wobec obu zbuntowanych republik wpisywały się w szerszy kontekst, nie tylko opisanej już polityki wobec obszaru poradzieckiego, ale również w logikę rywalizacji o wpływy z USA na samym Kaukazie. Osłabienie Gruzji poprzez uniezależnienie od niej Abchazji i Osetii Południowej leżało więc w oczywistym interesie Moskwy, która słusznie postrzegała ten kraj jako zwolennika amerykańskiej obecności w regionie. Zaostrzenie polityki rosyjskiej było zatem naturalną reakcją na bezprecedensową decyzję państw NATO w sprawie uznania niepodległości Kosowa.

Napięcia na linii Gruzja — Osetia Południowa — Rosja sięgnęły zenitu na początku sierpnia 2008 roku, kiedy zaczęło dochodzić do coraz częstszych starć na granicy. Sam konflikt zbrojny rozpoczął się 7 sierpnia 2008 roku o godzinie 23.30 masowym ostrzałem rakietowym Cchinwali przeprowadzonym przez Gruzinów, po którym nastąpiło uderzenie piechoty oraz sił pancernych. Stosunkowo szybko okazało się jednak, że plan Tbilisi na tę operację zaczął napotykać poważne problemy. Po pierwsze siły zbrojne Gruzji utknęły w stolicy Ose-

[78] *Exercise Helps Partner Nations Overcome Cultural Barriers*. U.S. Department of Defense: www.defense.gov/News/NewsArticle.aspx?ID=50608; dostęp: 20.12.2013; *Russia begins active stage of Caucasus 2008 military exercise*. Ria Novosti, 15.07.2008: http://en.ria.ru/world/20080715/114038236.html; dostep: 20.12.2013.

tii, mimo iż zakładano jej szybkie zdobycie. Po drugie nie udało się zaskoczyć sił rosyjskich, które natychmiast zareagowały na złamanie porozumienia z 1992 roku. Po trzecie zaatakowano batalion sił pokojowych Federacji Rosyjskiej, co dało Kremlowi wyraźny powód zaangażowania się w ten konflikt. Po czwarte fiaskiem zakończyły się próby zablokowania tunelu Roki, którym od 8 sierpnia 2008 roku napływały jednostki 58. armii. Istotnym elementem reakcji rosyjskiej poza wysłaniem sił lądowych było także rozpoczęcie bombardowań lotniczych, zarówno oddziałów gruzińskich w Osetii, jak i infrastruktury wojskowej w samej Gruzji. Skala popełnionych błędów, rosnąca dysproporcja sił, a także niskie morale oddziałów gruzińskich w konsekwencji nie pozwoliły na zrealizowanie założeń operacji wojskowej. Klęska stała się pewna w zasadzie już 9 sierpnia 2008 roku, kiedy *de facto* wojska gruzińskie przegrały bitwę o Cchinwali, dokonano ataku na Wąwóz Kodori z terenu Abchazji, a także do boju ruszyła rosyjska Flota Czarnomorska, dokonując blokady wybrzeża. W efekcie doprowadziło to do załamania oporu armii gruzińskiej, która zaczęła się bezładnie cofać w kierunku Gori, a później Tbilisi. W tej sytuacji od 11 sierpnia siły rosyjskie oraz separatystyczne zaczęły swobodnie operować po terytorium zachodniej i środkowej Gruzji. Po wycofaniu pozostałości oddziałów gruzińskich do stolicy wojna zakończyła się 12 sierpnia bezwarunkowym zwycięstwem Rosjan. Warto zauważyć, iż w zasadzie nie powiodły się międzynarodowe inicjatywy zmierzające do osiągnięcia zawieszenia broni. Co prawda Dmitrij Miedwiediew zgodził się na sześciopunktowy plan zaproponowany przez Nicolasa Sarkozy'ego, Federacja nie respektowała jednak jego ustaleń (Lakomy, 2010a: 182—184; szerzej: Nichol, 2009).

Z perspektywy omawianego tematu badawczego konflikt gruzińsko-rosyjski zyskał jednak pewną unikalną cechę. Jak stwierdził David Hollis (2011: 2), mógł być to pierwszy w historii przypadek skoordynowanego, szkodliwego wykorzystania cyberprzestrzeni z prowadzeniem operacji lądowych, powietrznych oraz morskich. Wynikało to z faktu, iż w wojnie tej, mającej z pozoru charakter wyłącznie konwencjonalny, istotną rolę odegrały właśnie sieci komputerowe. Warto więc podjąć próbę szerszego omówienia właściwości i znaczenia cyberataków w trakcie wydarzeń na Kaukazie, rozpoczynając od charakterystyki dwóch podstawowych zagadnień.

Przede wszystkim, w przeciwieństwie do Estonii, Gruzja jest państwem o stosunkowo niskim stopniu zaawansowania technologicznego, w którym dorobek rewolucji informatycznej nie był w 2008 roku jeszcze powszechnie stosowany. Świadczyły o tym najdobitniej dwa fakty. Po pierwsze w 2012 roku Gruzja zajmowała dopiero 71. miejsce w rankingu *ICT Development Index* Międzynarodowego Związku Telekomunikacyjnego, wyżej uplasowały się w nim takie kraje, jak Mołdawia, Bośnia i Hercegowina bądź Oman (*Measuring the Information Society*, 2013: 24). Po drugie statystycznie w 2008 roku w Gruzji było jedynie 9 użytkowników Internetu na 100 mieszkańców, czyli wielokrotnie

mniej w porównaniu do państw bałtyckich czy Europy Środkowej i Wschodniej[79]. Sytuacja ta miała dwojakie konsekwencje dla bezpieczeństwa teleinformatycznego Gruzji. Z jednej strony ze względu na niewielkie uzależnienie od ICT rząd w Tbilisi teoretycznie nie był zagrożony poważnymi incydentami w cyberprzestrzeni, z drugiej jednak w przypadku ich wystąpienia nie posiadał odpowiedniego potencjału technologicznego i eksperckiego, aby je skutecznie zatrzymać i zminimalizować poczynione szkody.

Drugim czynnikiem, na który warto zwrócić uwagę, było poważne uzależnienie gruzińskiej infrastruktury teleinformatycznej od Moskwy. Jak wskazali eksperci natowskiego Centrum Doskonalenia Cyberobrony (Cooperative Cyber Defence Center of Excellence), Gruzja była połączona z Internetem czterema kanałami: przez Turcję, Armenię, Azerbejdżan oraz Rosję, jednak niemal połowa z 13 kabli łączących ten kraj z siecią globalną biegła właśnie przez terytorium Federacji (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 6). Moskwa posiadała więc potencjalnie skuteczne instrumenty wywierania wpływu na funkcjonowanie gruzińskiego Internetu.

Pierwsze poważniejsze cyberataki między Rosją a Gruzją wystąpiły już na kilka tygodni przed rozpoczęciem wojny. Do pierwszego doszło prawdopodobnie 19 lipca, kiedy metodą DDoS zaatakowano witrynę internetową prezydenta Michaiła Saakaszwilego, skutkiem czego przez 24 godziny była ona niedostępna dla innych użytkowników sieci. Shadowserver Foundation analizując ten incydent, zauważyła, iż wykorzystano do tego kontrolowany zwyczajowo przez rosyjskich kryminalistów *botnet* Machbot (Ibidem, s. 36). W świetle późniejszych wydarzeń można się zastanawiać, czy nie był to wstępny test skuteczności wdrożonych przez rząd w Tbilisi rozwiązań. Do kolejnych incydentów doszło 5 sierpnia, kiedy zaatakowano strony internetowe agencji informacyjnej OS-Inform oraz OSRadio. Pierwsza z nich została zastąpiona materiałami pochodzącymi z portalu Alania TV, telewizji skierowanej do Osetyńczyków i wspieranej przez prezydenta Michaiła Saakaszwilego. Świadczyło to o tym, iż za cyberatakami stali Gruzini, którzy, jak zasugerował osetyński wysłannik do Moskwy Dmitrij Medojew, mogli chcieć w ten sposób zablokować informacje na temat kolejnych starć przygranicznych[80].

Do przełomu doszło jednak dopiero 8 sierpnia wraz z wybuchem konwencjonalnego konfliktu zbrojnego, w momencie uderzenia na Cchinwali rozpoczęła się bowiem zmasowana kampania cyberataków wymierzonych w najistotniejsze punkty gruzińskiego Internetu. Początkowo swoim zasięgiem objęła ona 54 witryny internetowe należące nie tylko do instytucji publicznych, takich jak Kancelaria Prezydenta, rząd czy poszczególne ministerstwa, ale także do pod-

[79] *Georgia in Figures*. One World Nations Online: www.nationsonline.org/oneworld/Country-Stats/Georgia-statistics.htm; dostęp: 20.12.2013.

[80] *S. Ossetian News Sites Hacked*. Civil.ge, 05.08.2008: www.civil.ge/eng/article.php?id=18896; dostęp: 20.12.2013.

miotów sektora prywatnego, w tym przede wszystkim przedsiębiorstw telekomunikacyjnych i finansowych (Hollis, 2011: 2—3). Listy najważniejszych celów ataków pojawiły się natychmiast na wielu rosyjskojęzycznych forach dyskusyjnych i były aktywnie rozpowszechniane przez internautów. Co ciekawe, incydenty te nie zakończyły się 12 sierpnia, wraz z rozstrzygnięciem sytuacji na froncie, już bowiem dzień później, jak podała Shadowserver Foundation, doszło do następnych zmasowanych ataków DDoS (typu ICMP), skierowanych przeciwko stronom rządowym w Tbilisi. Brały w nich udział przede wszystkim pojedyncze komputery, posiadające rosyjskie IP. Świadczyło to o tym, iż wykorzystano wówczas ogólnie dostępny w Internecie skrypt umożliwiający indywidualną partycypację w tym przedsięwzięciu. Po nich nastąpiły kolejne, o wiele poważniejsze ataki. Tym razem użyto prawdopodobnie aż 6 globalnych sieci *botnet*. Oprócz stron rządowych na cel wzięto wówczas także media elektroniczne. O skali ataków świadczył fakt, iż w największym natężeniu osiągnęły one poziom ponad 800 Mb/s i trwały ponad 6 godzin. Tego typu aktywność była kontynuowana aż do końca sierpnia 2008 roku. Ostatni poważny cyberatak wymierzony w Gruzję odnotowano 27 sierpnia po godzinie 16.00 czasu lokalnego. Wówczas na cel wzięto portal Ministerstwa Spraw Zagranicznych. W ciągu sekundy trafiało na niego wówczas ok. pół miliona pakietów danych. Na tym tle warto odnotować, iż stopniowe wygaszanie działań w cyberprzestrzeni wynikało z jednej strony ze stopniowej stabilizacji sytuacji na Kaukazie, z drugiej natomiast z zablokowania przez władze w Tbilisi adresów IP dotychczasowych sprawców (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 40—41; Clarke, Knake, 2010: 16; Nazario, 2009).

Znając ogólny przebieg wydarzeń, warto jednak dokonać bardziej szczegółowej analizy wykorzystanych wówczas metod. Przede wszystkim należałoby zauważyć, iż podobnie jak w przypadku Estonii odwołano się tu głównie do dwóch najpopularniejszych: *website defacement* oraz DoS/DDoS. W pierwszym przypadku włamano się do wielu witryn instytucji publicznych, w tym władz centralnych. Najbardziej oczywistym celem była strona prezydenta Gruzji Michaiła Saakaszwilego (www.president.gov.ge), której treść została zmodyfikowana w taki sposób, aby współgrać z wykładnią rosyjskiej propagandy wojennej: zamieszczono na niej przetworzone zdjęcia prezydenta Gruzji wraz z fotografiami Adolfa Hitlera. W ten sam sposób zamieniono treść innych ważnych portali, w tym m.in. Ministerstwa Spraw Zagranicznych czy Narodowego Banku Gruzji (www.nbg.gov.ge). Na stronie tego ostatniego pojawiła się nawet cała galeria dyktatorów XX wieku. Wśród nich jedno z miejsc zajmował właśnie Michaił Saakaszwili (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 6—7). Wpisywało się to w oficjalne stanowisko rządu Federacji Rosyjskiej, a także opinię rosyjskich mediów na temat konfliktu, które często przedstawiały władze w Tbilisi jako zbrodniarzy, nazistów lub faszystów. Oskarżenia takie sformułował np. minister spraw zagranicznych FR Siergiej Ławrow, wska-

zując, że Gruzini w trakcie walki popełnili zbrodnie wojenne[81]. W taki sposób o przebiegu konfliktu informował również popularny rosyjski portal Pravda.ru[82]. W związku z tym można zauważyć daleko idącą synergię między publikowanymi na zaatakowanych stronach gruzińskich materiałami a treścią oficjalnych komunikatów Kremla oraz mediów rosyjskich.

Oprócz metody *web defacement* podobnie jak w Estonii szeroko wykorzystano również techniki DoS/DDoS, których celem jest nie tyle podmiana zawartości strony WWW, co zablokowanie określonej usługi. W ten sposób zaatakowano m.in.: witryny prezydenta Gruzji, Ministerstwa Edukacji i Nauki (www.mes.gov.ge), parlamentu (www.parliament.ge), a także wybranych instytucji publicznych (takich jak www.naec.gov.ge). W tym przypadku cyberataki objęły również wiele portali należących do szeroko pojętego sektora prywatnego. Należy tu wskazać na największe gruzińskie forum dyskusyjne (www.forum.ge), największą anglojęzyczną stronę informacyjną (www.civil.ge), agencję prasową (www.presa.ge), portale informacyjne (www.apsny.ge, www.news.ge, interpress.ge, www.tbilisiweb.info, www.newsgeorgia.ru) oraz telewizję Rustavi 2 (www.rustavi2.com). Celem DDoS stały się także instytucje finansowe, w tym największy bank komercyjny (www.tbc.ge), a także inne, specyficzne witryny, w tym np. strona zrzeszająca gruzińskich hakerów i haktywistów: www.hacking.ge (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 8—9).

Szkodliwa aktywność w cyberprzestrzeni podczas tej wojny, oprócz *web defacement* i DDoS, obejmowała również i inne metody. Przede wszystkim za ekspertami CCD COE warto zwrócić uwagę na częste zastosowanie złośliwego oprogramowania. W rosyjskim Internecie w sierpniu 2008 roku pojawiły się pliki „war.bat", które stały się ogólnodostępne także dla internautów, którzy nie byli bezpośrednio związani ze środowiskiem haktywistów. Za ich pomocą każdy użytkownik miał możliwość partycypacji w atakach typu DDoS przeciwko wybranym gruzińskim instytucjom państwowym. Był to więc mechanizm znany już z Estonii z kwietnia i maja 2007 roku. Warto także zwrócić uwagę na fakt, iż na rosyjskich forach internetowych pojawiały się regularnie informacje na temat wykrytych luk w gruzińskich zabezpieczeniach, w tym np. wrażliwości na ataki typu *SQL injection*. W tym czasie pojawiła się również specjalna strona internetowa (www.stopgeorgia.ru), która udostępniała internautom rozmaite narzędzia przydatne do uczestniczenia w cyberatakach (głównie za pomocą metody DDoS) przeciwko rządowi gruzińskiemu (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 9—10). Ciekawym i przećwiczonym już sposobem szkodzenia w cyberprzestrzeni okazał się ponadto spam. W rosyjskim

[81] *Interview by Minister of Foreign Affairs of the Russian Federation Sergey Lavrov to BBC*. The Ministry of Foreign Affairs of the Russian Federation, Moscow, 09.08.2008: www.mid.ru/brp_4.nsf/0/F87A3FB7A7F669EBC32574A100262597; dostęp: 20.12.2013.

[82] Zob. *Georgia's Saakashvili commits war crimes against humanity*. Pravda.ru, 08.08.2008: http://english.pravda.ru/news/hotspots/08-08-2008/106045-georgia-0; dostęp: 20.12.2013.

Internecie stosunkowo szybko pojawiły się listy adresów e-mail najważniejszych gruzińskich polityków, na które masowo zaczęto wysyłać wiadomości. Celem tych działań było zablokowanie skrzynek elektronicznych najważniejszych osób w państwie. Szeroko rozpowszechniano wśród Gruzinów podrobione wiadomości elektroniczne zawierające złośliwe oprogramowanie. Jednym z najciekawszych przykładów może być sfałszowana informacja BBC, sugerująca, iż prezydent Michaił Saakaszwili był homoseksualistą. Do wiadomości jako dowód dołączano zainfekowany plik „name.avi.exe", którego otworzenie skutkowało zainfekowaniem komputera wirusem[83]. Zastosowanie tego typu środków świadczyło więc o dużym doświadczeniu sprawców w stosowaniu metod *phishingu*. Pojawiły się również niepotwierdzone informacje o tym, iż podjęto próbę swoistej „cyberblokady" Gruzji, która miała polegać na przekierowaniu całego ruchu sieciowego w tym kraju przez terytorium Federacji Rosyjskiej, do czego wykorzystano potencjał słynnej Russian Business Network (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 10—11). Można także wspomnieć o udanych próbach zablokowania zwyczajowych kanałów komunikacji wykorzystywanych przez środowisko ekspertów komputerowych w Gruzji (ibidem, s. 39). W ten sposób chciano zapobiec skoordynowanej odpowiedzi w cyberprzestrzeni ze strony Tbilisi. Było to zasadnicze *novum*, jeśli chodzi o tego typu operacje.

Na podstawie powyższych informacji powstaje jednak pytanie, kto był odpowiedzialny za te cyberataki oraz jakie były ich najważniejsze konsekwencje. Naturalne postrzegano je z reguły jako część toczącej się konwencjonalnej wojny między Gruzją a Rosją. Przedstawiciele rządu w Tbilisi, podobnie jak wcześniej Estończycy, nie mieli wątpliwości, iż za incydentami stały rosyjskie służby specjalne lub wojsko. Eka Tkeszelaszwili z gruzińskiej Rady Bezpieczeństwa Narodowego stwierdziła, iż „istnieje mnóstwo dowodów [wskazujących na fakt — M.L.], że ataki zostały bezpośrednio zorganizowane przez rząd Rosji". Jednocześnie jednak zastrzegła, iż nie są to informacje, które zostałyby uznane przez sąd. W innej z wypowiedzi zauważyła ona natomiast: „Rosja najechała Gruzję na czterech frontach. Trzy z nich były konwencjonalne — na ziemi, w powietrzu i na morzu. Czwarty był nowy — ich ataki w cyberprzestrzeni… Jest to po prostu nieprawdopodobne, aby równoczesne ataki na lądzie i w cyberprzestrzeni były przypadkiem"[84]. Również część analityków zwracała uwagę na wyjątkowy poziom koordynacji między działaniami konwencjonalnymi a aktywnością w sieci. John Bumgarner i Scott Borg zasugerowali, że na Kremlu podjęto decyzję, aby w trakcie konfliktu nie dokonywać zniszczeń gruzińskiej infrastruktury krytycznej, jednocześnie dając do zrozumienia państwom

[83] *Georgie: d'une cyber attaque*. Les Carnets Web de Thibaut, 11.12.2008: www.pagasa.net/georgie-recit-dune-cyber-attaque; dostęp: 2.01.2014.

[84] N. Schachtman: *Top Georgian Official: Moscow Cyber Attacked Us — We Just Can't Prove It*. „Wired" 03.11.2009: www.wired.com/dangerroom/2009/03/georgia-blames; dostęp: 3.01.2014.

zachodnim, że Federacja posiada takie zdolności. Świadczyły o tym jej działania wobec ropociągu Baku — Ceyhan. Lotnictwo rosyjskie wielokrotnie bombardowało jego okolice, nie trafiając jednak w samą instalację. Podobnie wyglądała strategia zastosowania środków teleinformatycznych, które nie tyle miały dokonać nieodwracalnych zniszczeń, co sprawić Tbilisi poważne problemy oraz ułatwić realizację rosyjskich interesów (Hollis, 2008: 4). Na oczywisty związek między Rosją a incydentami komputerowymi w sierpniu 2008 roku wskazywał również Jose Nazario z Arbor Networks. Stwierdził on, iż pakiety danych płynące do Gruzji zawierały wiadomość *win+love+in+Russia*. Rząd rosyjski zdecydowanie odcinał się od odpowiedzialności za ataki, mimo iż formalnie nie musiał tego czynić. Ambasador w Waszyngtonie Jewgienij Horiszko w rozmowie z dziennikarzami nie wykluczał natomiast, iż były one organizowane przez niezadowolonych z sytuacji na Kaukazie rosyjskich obywateli, haktywistów[85].

Rozstrzygnięcie kwestii odpowiedzialności za incydenty teleinformatyczne na Kaukazie wymagało pogłębionych badań, środowisko analityków komputerowych wskazywało bowiem z reguły na dwie grupy sprawców. Podobnie jak w przypadku Estonii z pewnością w cyberatakach brały udział szerokie rzesze rosyjskich haktywistów oraz amatorów (*script kiddies*), którzy na wybranych stronach internetowych oraz forach byli w stanie uzyskać narzędzia oraz informacje niezbędne do zaszkodzenia rządowi w Tbilisi online. Stali oni jednak tylko za częścią incydentów w cyberprzestrzeni z sierpnia 2008 roku, jak bowiem wskazano w wielu raportach poświęconych tym wydarzeniom, głównym podmiotem organizującym w sieci działania przeciwko Gruzji była, wspomniana już, Russian Business Network, kontrolowana prawdopodobnie przez dwóch Rosjan: Aleksandra A. Bojkowa oraz sławnego spamera Andrieja Smirnowa. Świadczył o tym fakt, iż źródłem wielu cyberataków były serwery i sieci kontrolowane lub powiązane z RBN. Jedna z francuskich analiz wskazała tu m.in. na dwa serwery C&C (*command & control*): bizus.kokovs.cc oraz ns1.guagaga.net[86]. Warto zauważyć, iż RBN była wówczas powszechnie uznawana za znaczącą organizację cyberprzestępczą, specjalizującą się w działalności kryminalnej w sieci, począwszy od propagowania pornografii, przez kradzież tożsamości użytkowników Internetu, organizowanie ataków DDoS, rozpowszechnianie szkodliwego oprogramowania, aż po hazard. Jak stwierdził David Bizeul w pracy opublikowanej w 2007 roku, RBN udostępniała kompleksową infra-

[85] J. Markoff: *Before the Gunfire, Cyberattacks*. „The New York Times" 12.08.2008: www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&n=Top/News/World/Countries%20and%20Territories/Russia&adxnnl=1&adxnnlx=1228825381-w2QRAeN708P9+3z2Zt5uYQ&; dostęp: 2.01.2014.

[86] *Georgie: d'une cyber attaque*. Les Carnets Web de Thibaut, 11.12.2008: www.pagasa.net/georgie-recit-dune-cyber-attaque; dostęp: 2.01.2014.

strukturę przydatną do zakazanej aktywności w cyberprzestrzeni[87]. W tym kontekście można wskazać na kilka znaczących przykładów działalności tej grupy:

- rozpowszechnienie złośliwego programu infekującego przeglądarki internetowe *CoolWebSearch* w 2005 roku,
- udział w cyberataku na stronę internetową Bank of India (metodą *web defacement*) w sierpniu 2007 roku,
- umieszczenie na swoich serwerach trojanów wymierzonych w sektor finansowy (banki),
- organizowanie ataków DDoS przeciwko instytucjom finansowym (np. National Australia Bank w październiku 2006 roku),
- masowe rozpowszechnianie spamu[88].

Tym samym Russian Business Network uznawano przed 2008 rokiem za profesjonalną i działającą globalnie rosyjską organizację przestępczą ograniczającą się wyłącznie do przestrzeni teleinformatycznej.

Powstaje więc pytanie, jaki interes miałaby tego typu grupa, aby mieszać się do konwencjonalnego konfliktu zbrojnego między Federacją Rosyjską a Gruzją. Z reguły takie podmioty unikają bezpośredniego uderzenia w instytucje państwowe, skupiając się raczej na sektorze prywatnym oraz pojedynczych internautach, bo to właśnie w nich upatrują głównych perspektyw uzyskania znacznych korzyści finansowych (Terlikowski, 2009: 96). Udział w cyberatakach przeciwko poszczególnym rządom oznaczałby natomiast uzasadnione ryzyko większego zainteresowania ze strony międzynarodowej opinii publicznej. Jedyną w zasadzie sensowną odpowiedzią na to pytanie mógł być fakt istniejących powiązań między Russian Business Network a rosyjskimi służbami specjalnymi. Możliwość taka była zresztą szeroko komentowana przez publicystów oraz ekspertów[89]. Wielu dziennikarzy zwracało uwagę, że rosyjskie władze z reguły bardzo pobłażliwie podchodziły do działalności tej organizacji, co mogło sugerować jakąś formę współpracy między nimi. Warto tutaj przytoczyć słowa Piotra Matyska, według którego

> działalność przychylnych Kremlowi crackerów to pewnego rodzaju symbioza. Kreml jest zadowolony, bo wskazuje cele ataku, pozostając w białych rękawiczkach — adresy IP atakujących wskazują na crackerów, a nie na rządową

[87] D. Bizeul: *Russian Business Network study*. Bizeul.org, 20.11.2007, s. 5: www.bizeul.org/files/RBN_study.pdf; dostęp: 2.01.2014.

[88] D. Bizeul: *Russian Business Network*…, op.cit., 5—10. Zob. także: B. Krebs: *Mapping the Russian Business Network*. „The Washington Post" 13.10.2007: http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html; dostęp: 2.01.2014.

[89] Zob. K. Flook: *Russia and the Cyber Threat*. Critical Threats, 13.05.2009: www.criticalthreats.org/russia/russia-and-cyber-threat; dostęp: 02.01.2013; *RBN — Georgia Cyberwarfare — Status and Attribution*. RBNExploit: http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-status-and.html; dostęp: 2.01.2013.

> instytucję, co doprowadziłoby niechybnie do skandalu. Crackerzy są zadowoleni, gdyż mogą robić to, co kochają najbardziej, będąc pewnymi, że nikt nie zapuka do drzwi. Oczywiście czasami może być potrzebna jakaś polityczna ofiara, ale to i tak niska cena. Trudno udowodnić, że grupy cyberprzestępców mają powiązania z FSB, na pewno służby specjalne starają się penetrować te środowiska. Ale gdyby takich kontaktów nie było, to czy działania RBN byłyby tak dobrze skoordynowane z działaniami wojska?[90].

Pojawiały się jednak i poważne głosy wątpiące w taką interpretację. Jednym z nich był *Virtual Criminology Report 2009* opracowany przez korporację McAfee. Przywołano w nim wyniki analizy wydarzeń z sierpnia 2008 roku przeprowadzonej przez niezależny instytut badawczy U.S. Cyber Consequences Unit (US-CCU). Stwierdzono w niej jednoznacznie, że cyberataki miały charakter *stricte* cywilny, choć ktoś z władz Federacji musiał przekazać haktywistom informację, kiedy rozpocznie się konflikt zbrojny (*Virtual Criminology Report*, 2009: 6).

Narastające wątpliwości w tej sprawie rozwiał dopiero *Grey Goose Phase II Report: The evolving state of cyber warfare* korporacji Greylogic, opublikowany 20 marca 2009 roku. Aby odpowiedzieć na pytanie, kto stał za cyberatakami przeciwko Gruzji, jej analitycy zbadali sposób funkcjonowania oraz powiązania wspomnianej już witryny internetowej www.stopgeorgia.ru. Już pierwsze rutynowe działania wykazały, iż założyciel tej strony był powiązany z innymi rodzajami przestępczej działalności w rosyjskiej cyberprzestrzeni, w tym m.in. fałszowaniem paszportów. Okazało się również, iż serwer, na którym powstała ta strona, należał do firmy SteadyHost, której siedziba znajdowała się w bezpośrednim sąsiedztwie dowództwa wywiadu wojskowego, Głównego Zarządu Rozpoznawczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Innym ciekawym aspektem tej sprawy były przytoczone przez Greylogic elementy doktryny cyberwojennej Rosji. Po pierwsze wskazano na przemówienie generała Aleksandra Burutina z lutego 2007 roku, w którym stwierdził, iż

> wyjątkowość broni informacyjnych wynika z tego, iż rozwijając swoją narodową infrastrukturę informacyjną, państwa tworzą bazę materialną dla użycia technologii informacyjnych do celów wojskowych. Im wyższy potencjał naukowy i techniczny, tym szersza [jest — M.L.] lista potencjalnych celów.

Po drugie przypomniano również artykuł w czasopiśmie „Moscow Military Thought", w którym zauważono:

---

[90] P. Matyska: *Russian Business Network — próba ustalenia faktów*. Portal Spraw Zagranicznych, 17.12.2009: www.psz.pl/RUSSIAN-BUSINESS-NETWORK-proba-ustalenia-faktow; dostęp: 2.01.2014.

> Z naszego punktu widzenia, wyodrębnienie cyberterroryzmu i cyberprzestępczości z szerszego kontekstu międzynarodowego bezpieczeństwa informacyjnego jest w pewnym sensie sztuczne i nie poparte jakąkolwiek obiektywną koniecznością […]. Co więcej, źródła cyberataków mogą być z łatwością wyposażone w legendę akcji przestępczych lub terrorystycznych[91].

Sugerowało to, iż na szczytach władzy w Moskwie dostrzegano możliwość powiązania działań cyberprzestępczych z realizacją określonych interesów poza granicami kraju, także podczas konfliktu zbrojnego. Na podstawie wszystkich dostępnych materiałów eksperci Greylogic jeszcze w październiku 2008 roku twierdzili jednak, iż nie znaleziono niezbitych dowodów na powiązania pomiędzy stroną stopgeorgia.ru a rosyjskimi służbami:

> Z wysokim stopniem pewności oceniamy, że rosyjski rząd będzie kontynuował swoją praktykę dystansowania się od rosyjskiego, nacjonalistycznego środowiska hakerskiego, zyskując możliwość zaprzeczenia [ewentualnym oskarżeniom — M.L.], jednocześnie pasywnie wspierając i ciesząc się ze strategicznych korzyści wynikających z ich akcji.

Nie wykluczono przy tym zarazem daleko idących powiązań między Kremlem a haktywistami. Sytuacja ta zmieniła się już na początku 2009 roku, kiedy w rosyjskich mediach pojawił się reportaż na temat sposobów wykorzystania przez Moskwę cyberataków do realizacji własnych interesów[92]. Zaprezentowane tam dowody przekonały specjalistów Greylogic do modyfikacji ich stanowiska, co poskutkowało tym, że w podsumowaniu raportu autorzy stwierdzili, iż „rosyjska polityka wojskowa uznaje strategiczne znaczenie […] cyberataków, które mogą wydawać się aktami cyberprzestępczości lub terroryzmu" oraz że forum stopgeorgia.ru było częścią przestępczej sieci, która została stworzona m.in. w celu zamaskowania zaangażowania FSB/GRU. Tym samym według omawianego opracowania ataki na gruzińską cyberprzestrzeń były zorganizowanymi przez Kreml operacjami informacyjnymi (*Information Operations*)[93].

Wykazanie pośredniego udziału rosyjskich służb specjalnych w tych wydarzeniach było istotnym osiągnięciem, gdyż potwierdzało wcześniejsze opinie wskazujące na wysoki stopień koordynacji i współzależności między oficjalnym stanowiskiem władz państwowych, konwencjonalnymi działaniami sił zbrojnych i cyberatakami[94], wyjaśniało ponadto powód, dla którego organizacja przestęp-

[91] Carr, Rios, Plansky, Walton, Devost, Moran, Givner-Forbes, Silverstein, 2009, s. 15—23.

[92] Ibidem, s. 20.

[93] Ibidem, s. 4.

[94] W jednej z analiz zwracano m.in. uwagę, skąd rosyjscy haktywiści wiedzieli, gdzie i kiedy uderzy armia Federacji. Świadczyło o tym np. zablokowanie witryn internetowych lokalnych władz oraz mediów w Gori, zanim dotarły tam pierwsze samoloty rosyjskie. Oznaczało to utratę możli-

cza zaangażowała się w nietypowe dla siebie akcje w Internecie, tym bardziej, iż w konsekwencji późniejsza działalność RBN została znacząco utrudniona. Na koniec zaś potwierdzało coraz wyraźniejszą praktykę wykorzystania przez FR potencjału technologii teleinformatycznych w relacjach z krajami strefy poradzieckiej.

Znając sprawców cyberataków, warto zastanowić się nad pośrednimi i bezpośrednimi reperkusjami tych działań. Przede wszystkim należy zauważyć, iż metody były bardziej zaawansowane niż w przypadku wydarzeń w Estonii. Korporacja McAfee poziom złożoności ataków z kwietnia i maja 2007 roku w skali od 1—10 oceniała na 1, tymczasem w przypadku Gruzji było to już 3. Jednocześnie jednak konsekwencje ataków dla gruzińskiej infrastruktury teleinformatycznej oceniono jako nieco mniejsze (*Virtual Criminology Report*, 2009: 9). Na Kaukazie nie wykorzystano co prawda żadnych unikalnych „cyberbroni" lub nieznanych dotąd sposobów włamań, zastosowano natomiast na masową skalę przećwiczone już wcześniej metody, które w pełni się sprawdziły. Wynikało to przede wszystkim z niskiego poziomu rozwoju technologicznego samej Gruzji. Świadczyły o tym najlepiej czasowe utrudnienia funkcjonowania krajowych dostawców usług internetowych (ISP), oznaczające *de facto* odcięcie części obywateli od globalnej sieci. Z tego typu problemami zetknęły się m.in. routery United Telecom of Georgia oraz Caucasus Network. Sytuacja ta dodatkowo pogłębiła i tak wyraźny chaos informacyjny w kraju. Na brak podstawowych zabezpieczeń komputerowych wskazywała także decyzja Narodowego Banku Gruzji o zablokowaniu na 10 dni świadczonych przez siebie usług elektronicznych (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 15—16). Z punktu widzenia bezpieczeństwa narodowego Gruzji oraz dynamiki konfliktu zbrojnego były to jednak kwestie raczej o marginalnym znaczeniu.

Za sprawę zdecydowanie ważniejszą należy uznać sytuację, w której *de facto* zablokowano Tbilisi możliwość prezentowania swojego stanowiska międzynarodowej opinii publicznej za pomocą Internetu. Było to wyjątkowo kłopotliwe, Michaił Saakaszwili od początku bowiem zabiegał o zaangażowanie Zachodu w ten konflikt. Bez podstawowych środków polityki informacyjnej starania te były znacząco utrudnione. Doprowadziło to w efekcie do kompromitującej dla Gruzji decyzji, aby zwrócić się o pomoc do innych państw oraz korporacji transnarodowych. Wspomniany już największy gruziński portal anglojęzyczny www.civil.ge ze względu na regularne ataki DDoS zdecydował się np. na wykorzystanie kontrolowanej przez Google platformy Blogspot. Jim Stogdill skomentował ten ruch następująco: „w pewnym sensie oni muszą mówić: nie możemy utrzymać naszych stron, ale nie sądzimy, aby [rosyjscy hakerzy — M.L.] byli w stanie zablokować Blogspot, wiedząc, że Google ma zdecydowanie lepszą infra-

wości skutecznego komunikowania z obywatelami, a więc i stabilizowania sytuacji wewnętrznej na danym obszarze, pogłębiało również wszechobecny chaos. Zob. Hollis, 2011: 5—6.

strukturę oraz zdolności do jej obrony”[95]. Innym przejawem niesamodzielności gruzińskich wysiłków na rzecz zabezpieczenia narodowej cyberprzestrzeni był fakt pomocy, jaką Tbilisi uzyskało od podobnie doświadczonej w tym względzie Estonii, w trakcie wojny Tallin zdecydował bowiem o udostępnieniu swoich serwerów gruzińskiemu Ministerstwu Spraw Zagranicznych, wysłano ponadto na Kaukaz dwóch specjalistów pracujących w estońskim zespole CERT[96]. Można także wskazać na szereg innych przykładów wsparcia społeczności międzynarodowej dla Michaiła Saakaszwilego. Na poziomie państwowym oprócz Estonii ograniczonej pomocy udzieliły Polska oraz Francja. W przypadku RP pomoc miała dwojaki charakter. Z jednej strony Kancelaria Prezydenta już 10 sierpnia umożliwiła władzom gruzińskim skorzystanie z witryny www.president.pl, gdzie mogły one zamieszczać najważniejsze informacje i deklaracje na temat toczącego się konfliktu zbrojnego. Jak stwierdzono w jej komunikacie, wynikało to z zablokowania strony gruzińskiego Ministerstwa Spraw Zagranicznych[97]. Z drugiej strony pomocy udzieliło również CERT Polska, które rozpoczęło analizę IP sprawców cyberataków. W przypadku Francji należy z kolei wskazać na zespół CERT, który pomógł Gruzinom zbierać niezbędne dane o incydentach teleinformatycznych (Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 15). Znaczną rolę w tych przedsięwzięciach odegrały także przedsiębiorstwa zachodnie. Jednym z nich było Tulip Systems (TSHost), amerykańska firma z Atlanty, która już 8 sierpnia zaoferowała Tbilisi udostępnienie własnej infrastruktury w celu ustabilizowania funkcjonowania rządowych stron internetowych, w rezultacie część z nich już następnego dnia znalazła się na serwerach w USA. Co ciekawe, nawet wówczas były one obiektem ataków typu DDoS z terytorium Federacji Rosyjskiej (Korns, Kastenberg, 2008: 66—67).

W tym kontekście konsekwencje paraliżu gruzińskiej cyberprzestrzeni trafnie ujął przytaczany już raport korporacji McAfee, w którym stwierdzono, iż „Rosja osiągnęła znaczące zwycięstwo psychologiczne, blokując Gruzji [możliwość — M.L.] rozpowszechniania precyzyjnych informacji o sytuacji wojennej […]. Co więcej, gdy gruzińska wersja wydarzeń została uciszona, Rosja praktycznie wygrała bitwę o międzynarodową opinię publiczną” (*Virtual Criminology Report*, 2009: 6). Warto również przytoczyć słowa Freda Schreiera (2015: 112), który w następujący sposób omówił te incydenty:

[95] Za: N. Shachtman: *Estonia, Google Help ‘Cyberlocked’ Georgia (Updated)*. „Wired” 11.08.08: www.wired.com/dangerroom/2008/08/civilge-the-geo; dostęp: 20.12.2013.

[96] R. Stiennon: *Estonia sending cyber defense experts to Georgia*. Network World, 11.08.08: www.networkworld.com/community/node/30935; dostęp: 20.12.2013.

[97] S. Górski: *Gruzja zaatakowana przez Rosję — również w Internecie*. „PC World” 11.08.2008: www.pcworld.pl/news/162227/Gruzja.zaatakowana.przez.Rosje.rowniez.w.Internecie.html; dostęp: 5.01.2013.

> Szybkość działań oraz wielokierunkowa natura tych cyberuderzeń wpisała się w klasyczną technikę wojskowego *swarmingu*, miażdżąc cyberobronę gruzińskich celów. Atakujące siły były wysoce zdecentralizowane, jednak zdolne do synchronizacji oraz koncentrowania ich operacji w sposób, który sprawiał, że gruzińska odpowiedź obronna była niemal niemożliwa. Głównym celem tej cyberkampanii było wsparcie rosyjskiej inwazji na Gruzję, a cyberataki zgrabnie wpasowały się w militarny styl napaści. Wiele z tych cyberuderzeń było wyraźnie przygotowanych po to, aby Gruzinom trudniej było zrozumieć, co się dzieje. Niezdolność Gruzinów do utrzymania ich stron internetowych niszczyło narodowe morale. Te ataki służyły również opóźnieniu międzynarodowej reakcji na konflikt kinetyczny.

W ciekawy sposób do tego zagadnienia odniósł się również David J. Smith (2012: 2), analityk Potomac Institute for Policy Studies, którego zdaniem w 2008 roku Rosja, łącząc cyberataki z uderzeniami kinetycznymi, zdobyła świetny materiał doświadczalny. Zauważył on ponadto, iż nie wykorzystano wówczas pełnego potencjału Federacji w tej dziedzinie. Mimo że bezpośrednie skutki cyberataków były nieco mniejsze niż w przypadku Estonii, ich wydźwięk dla propagandy wojennej oraz działań informacyjnych prowadzonych przez obie strony był nie do przecenienia.

Powyższe rozważania dają więc podstawę do stwierdzenia, iż cyberprzestrzeń odegrała istotną rolę w konflikcie gruzińsko-rosyjskim na Kaukazie w sierpniu 2008 roku. Analizując ten przypadek jako przejaw rywalizacji i konfrontacji państw w nowej domenie, jaką jest globalna sieć, można tu zwrócić szczególną uwagę na kilka spraw. Przede wszystkim należy podkreślić, że rosyjskie cyberataki przeciwko Gruzji spełniły warunki uznania jej za przejaw ograniczonej cyberwojny. Mimo mniejszego zagrożenia dla infrastruktury krytycznej państwa w porównaniu z *casusem* Estonii tym razem udział służb specjalnych w tych incydentach został potwierdzony przez raport Greylogic. Oprócz niego na powiązania między RBN a organami siłowymi FR wskazywały także inne scharakteryzowane wyżej przesłanki. Tym samym działania w przestrzeni teleinformatycznej w pewnym sensie rzeczywiście stały się piątym teatrem działań zbrojnych[98]. Różnica w stosunku do ujęć doktrynalnych zaprezentowanych w poprzednim rozdziale polegała na tym, iż cyberataki nie były raczej wymierzone w elementy infrastruktury krytycznej państwa czy systemy wojskowe, lecz w środki prowadzenia polityki informacyjnej, były zatem elementem walki informacyjnej, w której zasadniczą rolę odgrywa propaganda wojenna. Z perspektywy gruzińskiej oznaczało to ograniczenie możliwości prezentowania swojego

[98] Przy czym eksperci natowskiego CCD COE stwierdzili, iż istniała zasadnicza trudność zastosowania w tym przypadku prawa konfliktów zbrojnych, co ich zdaniem wynikało z trudności w jednoznacznym ustaleniu podstawowych faktów. Zob. Tikk, Kaska, Rünnimeri, Kert, Tailhärm, Vihul, 2008: 23.

stanowiska międzynarodowej opinii publicznej, co w zasadniczym stopniu ułatwiło zadanie dyplomacji rosyjskiej, która umiejętnie wykorzystała słabość polityki krajów zachodnich, częstokroć zajmujących dwuznaczne stanowisko wobec wydarzeń na Kaukazie. Przejawem tego stanu rzeczy było podpisanie sześciopunktowego porozumienia o zawieszeniu broni, którego Kreml od początku nie przestrzegał. Mimo to nie doszło do długotrwałego załamania relacji na linii UE/NATO — Rosja (Lakomy, 2010a: 192—194).

W szerszej perspektywie wykorzystanie cyberataków przez Rosję przyczyniło się do osiągnięcia oczekiwanych rezultatów politycznych, zarówno w wymiarze regionalnym, jak i globalnym. W pierwszym przypadku Moskwa udowodniła, iż nadal jest głównym rozgrywającym na Kaukazie, skutecznie tłumiąc prozachodnie aspiracje Michaiła Saakaszwilego. Wraz ze zwycięstwem w konflikcie zbrojnym ambicje Tbilisi, aby zostać członkiem NATO, zostały skompromitowane (Nichol, 2009: 11—12), tym bardziej, iż oprócz porażki militarnej państwo to pokazało, że nie potrafiło zapewnić podstawowego zakresu ochrony infrastrukturze teleinformatycznej. Moskwa umocniła dzięki temu swoje wpływy w Osetii Południowej oraz Abchazji, rewanżując się Zachodowi za uznanie niepodległości Kosowa. W wymiarze globalnym natomiast skutecznie osłabiono wpływy amerykańskie w regionie, udowadniając, iż współpraca polityczna i wojskowa z USA nie jest wystarczającym środkiem zapewnienia bezpieczeństwa narodowego. Mimo czasowego zerwania współpracy na linii NATO — Rosja to Zachód ostatecznie był zmuszony zainicjować ponowne zbliżenie, co wynikało głównie ze znaczenia Federacji dla misji ISAF w Afganistanie (Lakomy, 2010a: 190—199). Odnosząc to do typologii celów polityki zagranicznej ze wstępu, można więc zauważyć, iż cyberataki przyczyniły się w pewnym, choć zróżnicowanym stopniu, do realizacji trzech ogólnych priorytetów w działalności zewnętrznej Rosji: wzrostu siły państwa, wzrostu jego pozycji międzynarodowej oraz zapewnienia bezpieczeństwa. Z tych trzech cyberprzestrzeń odegrała największą rolę w realizacji drugiego, czyli wzmocnienia pozycji międzynarodowej kraju, ponieważ dzięki zablokowaniu polityki informacyjnej Tbilisi Kreml miał zdecydowanie prostsze zadanie, aby przedstawić swoją wersję wydarzeń na Kaukazie światowej opinii publicznej.

Reasumując, można przywołać zdanie zawarte w raporcie korporacji McAfee, w którym stwierdzono, że „zdolności cyberataków może nie są jeszcze główną bronią w arsenałach państw, jednak wydarzenia [te — M.L.] pokazały, że rosnąca liczba państw postrzega je jako część panoplii militarnej potęgi" (*Virtual Criminology Report*, 2009: 10). W podobny sposób wojnę na Kaukazie ocenił Lesley Swanson (2010: 303—304), według którego potwierdziła ona, iż ataki komputerowe stają się symbolem nowoczesnej wojny. Jego zdaniem

> walka składa się już nie tylko z ataków fizycznych bądź inwazji [dokonywanych — M.L.] pomiędzy nacjami przez odrębne jednostki wojskowe. Ten

> nowy sposób walki wykorzystuje technologię wziętego na cel narodu przeciwko niemu w celu osłabienia mającej żywotne znaczenie infrastruktury. Wraz z rozwojem Internetu oraz technologii komputerowych rozwijają się również metody i środki walki. […] rosyjsko-gruziński cyberkonflikt w 2008 roku ukazał, jak państwa coraz mocniej angażują się w cyberataki jako sposób osłabienia infrastruktury krytycznej przeciwnika — systemów i majątku o żywotnym znaczeniu dla bezpieczeństwa narodowego, bezpieczeństwa gospodarczego oraz zdrowia publicznego.

Można się również zgodzić z opinią Jamesa A. Lewisa, który stwierdził, iż wojna na Kaukazie unaoczniła, że cyberataki raczej będą instrumentem komplementarnym, a nie zastępującym konwencjonalne siły zbrojne (Lewis, 2011: 2). Na tym tle należy podkreślić, iż cyberprzestrzeń rzeczywiście odegrała ważną rolę w konflikcie gruzińsko-rosyjskim w sierpniu 2008 roku, osiągając skalę ograniczonej cyberwojny. Masowe ataki komputerowe przeprowadzane przez haktywistów oraz inspirowane przez służby rosyjskie organizacje przestępcze wsparły konwencjonalne działania zbrojne oraz wysiłki dyplomatyczne Kremla, aby starcie rozstrzygnąć na swoją korzyść. W kluczowych momentach, skutecznie blokując Tbilisi możliwość informowania międzynarodowej opinii publicznej o wydarzeniach na Kaukazie, Kreml w znacznym stopniu wzmocnił swoją pozycję negocjacyjną. Tym samym użycie instrumentów teleinformatycznych podniosło skuteczność realizacji podstawowych celów polityki zagranicznej Rosji, zarówno wobec strefy poradzieckiej, jak i szerzej: wobec Europy Zachodniej oraz Stanów Zjednoczonych.

4.4. Cyberataki w stosunkach na linii Rosja — Kirgistan

Ostatnim przypadkiem masowych cyberataków na obszarze poradzieckim, na który warto zwrócić uwagę, jest z pewnością *casus* Kirgistanu. Badając to zagadnienie, warto więc rozpocząć od charakterystyki podstawowych uwarunkowań jego relacji z Rosją. Z perspektywy Biszkeku z jednej strony były one determinowane doświadczeniami historycznymi, w tym przede wszystkim długotrwałym podporządkowaniem najpierw caratowi, a później Związkowi Socjalistycznych Republik Radzieckich (Akayev, 1994: 11; *Kyrgyzstan Country Profile*, 2009). Z drugiej jednak warto zauważyć, iż Kirgistan po rozpadzie ZSRR pozostał w strefie wpływów rosyjskich. W przeciwieństwie do innych krajów obszaru poradzieckiego tamtejsze władze w latach 90. XX wieku były mocno zainteresowane utrzymaniem jak największej obecności Moskwy w Azji Centralnej. Już w pierwszej połowie tej dekady prezydent Askar Akajew dążył do

zacieśnienia stosunków dwustronnych z Kremlem. Przejawiało się to zainicjowaniem szeregu przedsięwzięć gospodarczych, którymi jednak Rosjanie byli zainteresowani tylko w niewielkim stopniu, co w dużej mierze wynikało ze złej sytuacji gospodarczej tego kraju (zob. Collins, 2006: 188). O przyjaznej Federacji polityce świadczyło również poparcie dla projektu Unii Euroazjatyckiej sformułowanego w 1994 roku czy przyznanie językowi rosyjskiemu statusu języka urzędowego. Wszystkie te działania miały na celu ścisłe powiązanie Kirgistanu z FR, co wynikało zarówno z potrzeb ekonomicznych, jak i z niestabilności Azji Centralnej[99]. Należy pamiętać, iż Rosja była dla Biszkeku największym partnerem handlowym: w 2009 roku 11% eksportu i 36% importu przypadało właśnie na nią, a zasadniczą rolę odgrywały tu m.in. surowce energetyczne. Ponadto słaba pozycja Kirgistanu w stosunku do innych państw regionu sprawiała, że głównie we współpracy z Moskwą jego władze upatrywały sposobu na zapewnienie bezpieczeństwa narodowego[100]. Warto w tym kontekście przytoczyć zdanie sformułowane przez prezydenta Akajewa, które w pełni oddawało filozofię polityki rosyjskiej Biszkeku: „małe państwa potrzebują dużych przyjaciół" (Huskey, 2008: 5).

Polityka Moskwy wobec Kirgistanu wiązała się z nieco innymi założeniami. Przede wszystkim, jak wspomniano, wpisywała się w logikę stosunków z „bliską zagranicą". Początkowo zbliżenie z Biszkekiem było postrzegane jako udany przykład realizacji tej strategii, wzmacniający obecność Federacji w Azji Centralnej. Ponadto związki z tym krajem wynikały z niechęci do przyjmowania rosnącej imigracji diaspory rosyjskiej. Dlatego też zabiegano o nadanie rosyjskiemu statusu języka urzędowego, co miało pozwolić na powstrzymanie niekontrolowanego przepływu ludności w kierunku Federacji. Bez względu na to znaczenie Kirgistanu w polityce rosyjskiej w latach 90. XX wieku było jednak niewielkie[101]. Optyka ta zmieniła się dopiero na przełomie XX i XXI wieku, co wiązało się z dwoma wydarzeniami. Pierwszym z nich było dojście do władzy Władimira Putina, który ponownie zainteresował się Azją Centralną. Ruch ten wynikał z coraz bardziej agresywnej polityki Stanów Zjednoczonych wobec krajów dotychczas blisko związanych z Federacją, czego wyrazem była interwencja w Kosowie. Warto tu przytoczyć słowa Kubungazy'ego Bugubajewa, którego zdaniem „Rosja chciała sprzeciwić się rosnącym zachodnim wpływom w Azji Centralnej, sugerując, iż wykorzysta zarówno środki bila-

[99] Zob. *Kazakstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan: country studies*. Ed. G.E. Curtis. Washington, D.C. 1997: http://lcweb2.loc.gov/frd/cs/kgtoc.html; dostęp: 6.01.2014.

[100] E. Troitskiy: *Turmoil in Kyrgyzstan: A Challenge to Russian Foreign Policy*. The Swedish Institute of International Affairs, 30.01.2012, s. 11: www.ui.se/eng/upl/files/79297.pdf; dostęp: 06.01.2014.

[101] K. Bugubajew: *Kyrgyzstan-Russian Relations*. Strategic Outlook, May 2013, s. 2: http://strategicoutlook.org/publications/Kyrgyzstan_Russia_Relations.pdf; dostęp: 6.01.2014.

teralne, jak i multilateralne do powstrzymania wpływów Stanów Zjednoczonych […], aby stworzyć pas „dobrych sąsiadów" przy linii swoich granic"[102]. Drugim powodem większego nacisku na stosunki z Kirgistanem były obawy dotyczące rozpowszechnienia fundamentalizmu islamskiego w strefie poradzieckiej. Ze względu na konflikt w Czeczenii, narastającą destabilizację Afganistanu czy działalność Islamskiego Ruchu Uzbekistanu, znaczenie Biszkeku dla Moskwy w zasadniczym stopniu wzrosło. W tym kontekście Rosjanie postrzegali współpracę z tym krajem jako skuteczny środek powstrzymania proliferacji ekstremizmu religijnego, a także przepływu narkotyków oraz uchodźców w kierunku swoich granic[103].

Do dalszego podniesienia rangi Kirgistanu w polityce zagranicznej Rosji doszło po 11 września 2001 roku w wyniku zamachów terrorystycznych na World Trade Center, wraz ze zbliżającą się interwencją amerykańską w Afganistanie państwa zachodnie uznały bowiem ten kraj za obszar o strategicznym znaczeniu dla „wojny z terroryzmem". Warto tutaj przytoczyć słowa Euegene'a Huskeya (2008: 11), którego zdaniem „Zachód miał teraz nowy i bardziej pociągający powód zaangażowania w Kirgistanie. Nie był to już tylko nieudany eksperyment [związany — M.L.] z demokratyzacją, ale partner w walce antyterrorystycznej, walce skoncentrowanej wokół Afganistanu". W efekcie, jak wskazał autor, USA uzyskało w grudniu 2001 roku zgodę na zlokalizowanie swojej bazy wojskowej nieopodal stolicy. W zamian Biszkek uzyskał dodatkowe środki finansowe z Zachodu oraz umocnił swoją pozycję jako „pomost" między Wschodem a Zachodem. Przyczyniło się to jeszcze do większego zainteresowania tym krajem ze strony Kremla, który był zaniepokojony wzrastającymi wpływami USA. Dzięki temu podjęto działania, których celem było ponowne zlokalizowanie na jego terytorium wojsk rosyjskich. Ostatecznie siły powietrzne FR zostały rozmieszczone w miejscowości Kant, na wschód od stolicy (Nichol, s. 2). Chociaż początkowo Rosjanie nie wyrażali sprzeciwu wobec funkcjonowania bazy amerykańskiej w Azji Centralnej, z czasem jednak obecność sił USA zaczęła rodzić coraz większe wątpliwości.

Na tym tle, warto odwołać się do badań Jegwienija Troitskiego, który wyróżnił szereg celów polityki zagranicznej Rosji wobec Kirgistanu. Przede wszystkim wymienił on stabilizację tego kraju, przez co rozumiał złagodzenie problemów i tarć wewnętrznych, a także przeciwdziałanie wyzwaniom transnarodowym (tranzyt narkotyków, fundamentalizm islamski), ponieważ chaos w jego granicach oznaczałby dla Moskwy komplikacje w całym obszarze Azji Centralnej, w tym m.in. w Uzbekistanie oraz Tadżykistanie. Po drugie Kreml pragnął, aby Kirgistan pozostał lojalnym partnerem Federacji oraz członkiem zdominowanych przez nią struktur ponadnarodowych. Po trzecie chciano utrzymać znajdujące się w tym państwie rosyjskie instalacje wojskowe. Innym jesz-

[102] Ibidem, s. 5—6.
[103] Ibidem, s. 6.

cze priorytetem było zachowanie *status quo*, jeśli chodzi o sytuację mniejszości słowiańskiej na tym obszarze[104]. Do wskazanych wyżej celów należy jeszcze dodać zagadnienia związane z obecnością sił natowskich w bazie Manas, które rodziły w Moskwie coraz większe wątpliwości, obawiano się bowiem, iż będzie to stanowić swoisty punkt wyjścia do dalszych działań, których celem byłoby wyparcie wpływów rosyjskich z tego regionu. Potwierdzeniem takiej optyki wydarzeń była jedna z wypowiedzi ministra spraw zagranicznych Rosji Igora Iwanowa, który zauważył na początku XXI wieku, że Federacja będzie musiała stworzyć długotrwałe więzy ekonomiczne, szkolić kadry, udzielać kredytów, a także wspierać współpracę wojskową z państwami Azji Centralnej. W przeciwnym wypadku, jego zdaniem „próżnia ta zostanie wypełniona przez innych", czyli w domyśle przez USA[105].

Obawy z tym związane uwidoczniły się w marcu 2005 roku, kiedy doszło w Kirgistanie do „tulipanowej rewolucji", w której wyniku dotychczasowy prezydent Askar Akajew został obalony i zastąpiony przez Kurmanbeka Bakiewa. Na Kremlu wydarzenia te zinterpretowano jako kolejną „kolorową" rewoltę inspirowaną przez amerykańskie służby specjalne, których celem było osłabienie wpływów rosyjskich w strefie poradzieckiej. Stosunkowo szybko ten sposób postrzegania przewrotu został jednak zarzucony, gdyż nowy przywódca państwa zdecydował się na politykę przychylną wobec Federacji oraz ChRL. Nie zmieniło to jednak nadal niechętnego stanowiska Moskwy wobec amerykańskiej obecności w tym kraju, czego wyrazem była deklaracja Szanghajskiej Organizacji Współpracy z lipca 2005 roku, w której wezwano Biały Dom do określenia ostatecznej daty zamknięcia swojej bazy. Temat ten podchwycił sam Bakiew, który stwierdził, że w sytuacji postępującej stabilizacji Afganistanu należałoby dokonać przeglądu celowości jej istnienia. Wywołało to ożywioną reakcję amerykańskiej dyplomacji, niedługo bowiem później Biszkek odwiedził amerykański sekretarz obrony Donald Rumsfeld, który zapowiedział zwiększenie opłat za możliwość korzystania z lotniska Manas, co pozwoliło na dalsze funkcjonowanie bazy. Co ciekawe, zaczęła ona jednak wywoływać coraz większe kontrowersje wewnętrzne. Wynikały one z kilku powodów. Po pierwsze z obaw, że może ona zostać wykorzystana w celach bezpośrednio niezwiązanych z wojną z terroryzmem, w tym np. do ataku na Iran. Po drugie sprzeciw budził fakt, iż wyłączność na kontrakty do obsługi lotniska miały przedsiębiorstwa związane z obozem władzy. Po trzecie coraz większy opór budziła bezkarność amerykańskich żołnierzy (jeden z nich w grudniu 2006 roku zabił obywatela Kirgistanu, a następnie bez przeszkód powrócił do USA). Jak zauważył Eugene Huskey (2008: 12—13), rosyjska baza w Kant nie wywoływała aż takich napięć.

[104] E. Troitskij: *Turmoil in Kyrgyzstan*…, op.cit.
[105] K. Bugubajew: *Kyrgyzstan-Russian Relations*…, op.cit., s. 7.

Mimo przejściowego uregulowania tych kwestii w kolejnych latach napięcia związane z bazą narastały, do czego przyczyniały się miejscowe oraz rosyjskie media, które wskazywały na niekorzystny wpływ obecności wojsk zachodnich na środowisko naturalne. Takie hasła popierały niektóre prorosyjskie siły polityczne w kraju, w tym m.in. Partia Komunistów Kirgistanu, która organizowała nawet antyamerykańskie demonstracje (Nichol, s. 5). W tym kontekście problem lotniska amerykańskiego zaczął być poruszany na najwyższym szczeblu w kontaktach na linii Moskwa — Biszkek. Gdy w 2007 roku Rosja wprowadziła nowe prawo, które ograniczało możliwość podejmowania pracy przez imigrantów, sprzeciwiające się temu władze Kirgistanu zaoferowały w zamian za jego zniesienie zamknięcie lotniska w Manas. Niedługo później, w sierpniu, Władimir Putin zasugerował, iż istnieje możliwość zainwestowania w tym kraju 2 mld dolarów, czemu według rosyjskich mediów miał towarzyszyć nieformalny wymóg usunięcia wojsk zachodnich z jego terytorium. Miał to być także warunek udzielenia kolejnych pożyczek na sumę ok. 300 mln dolarów. Trzeba jednak przy tym zaznaczyć, iż te doniesienia zostały zdementowane przez obie strony. Niemniej już 3 lutego 2009 roku Kurmanbek Bakiew w trakcie swojej oficjalnej wizyty w Moskwie sam zapowiedział zamknięcie bazy, wskazując trzy powody tej decyzji: pierwszym była niedostateczna rekompensata za jej użytkowanie ze strony Waszyngtonu, drugim narastający sprzeciw ze strony obywateli, trzecim zakończenie operacji antyterrorystycznych w Afganistanie. W trakcie tej samej wizyty prezydent Miedwiediew zapowiedział daleko idące inwestycje w Kirgistanie. Odnosząc się do nerwowych reakcji państw zachodnich, przywódca Rosji stwierdził również, iż może ona zrekompensować NATO zamknięcie lotniska, umożliwiając mu transport niebojowych materiałów dla ISAF drogą lądową. W rezultacie podjętych decyzji 19 lutego 2009 roku parlament Kirgistanu przyjął ustawę, zgodnie z którą Stany Zjednoczone miały przekazać kontrolę nad lotniskiem Manas w ciągu następnych sześciu miesięcy. W kwietniu tego roku podobne akty wydano wobec korzystających z bazy pozostałych państw natowskich (Nichol, s. 5—6; *Kyrgyzstan Country Profile*, 2009: 30—37).

Decyzja władz Kirgistanu wywołała oczywiście poważne kontrowersje w samym Waszyngtonie. Politykę Kremla skrytykował m.in. sekretarz obrony USA Robert Gates[106]. Amerykanie podjęli jednak starania, aby decyzję Kirgistanu zmienić, co częściowo się udało. W wyniku dwustronnych negocjacji 23 czerwca 2009 roku osiągnięto porozumienie, którego istotą było potrojenie opłat za korzystanie z Manas oraz zmiana charakteru obecności US Air Force. Zgodnie z umową amerykańska część zmieniła status z bazy lotniczej na centrum logistyczne, nad którym kontrolę miały sprawować siły kirgiskie[107].

[106] *Kyrgyz Parliament Approves U.S. Base Closure*. Foxnews, 19.02.2009: www.foxnews.com/story/2009/02/19/kyrgyz-parliament-approves-us-base-closure; dostęp: 10.01.2014.

[107] *Kyrgyzstan Raises Rent On U.S. Air Base*. CBSNews, 23.06.2009: www.cbsnews.com/news/kyrgyzstan-raises-rent-on-us-air-base; dostęp: 10.01.2014.

Nawiązując do postawionego we wstępie celu badawczego, w dyskusji na temat losu amerykańskiej bazy wojskowej pewną rolę odegrała cyberprzestrzeń, na początku 2009 roku bowiem w Kirgistanie doszło do całej serii incydentów teleinformatycznych. Dokonując analizy tych wydarzeń, warto jednak na początek zwrócić uwagę na stopień rozwoju technologicznego tego państwa, który podobnie jak w przypadku Gruzji był stosunkowo niski. W 2008 roku w kraju było co prawda 3,4 mln telefonów komórkowych[108], jednak dostęp do sieci komputerowych był niewielki. Jedynie ok. 550 000 obywateli mogło korzystać z Internetu. Dodatkowo jego użytkowanie było w tym okresie stosunkowo drogie, a infrastruktura teleinformatyczna mało rozwinięta. Warto przywołać opinię Tattu Mambetalievy oraz Zlaty Shramko, które wskazały na kilka czynników wpływających na charakter rewolucji informatycznej w Kirgistanie. Wyróżniły one:

- uwarunkowania geograficzne związane z przewagą obszarów górzystych, z czym wiążą się utrudnienia oraz wysokie koszty rozbudowy infrastruktury teleinformatycznej,
- wysoki stopień koncentracji usług telekomunikacyjnych w Biszkeku (ok. 80% w skali kraju), podczas gdy mieszka tam jedynie 20% populacji,
- niskie zagęszczenie linii telefonicznych w obszarach wiejskich,
- nieproporcjonalny rozwój sieci internetowej związany z faktem, iż biedniejsze, oddalone od stolicy tereny zdecydowanie rzadziej są zainteresowane jej wykorzystaniem,
- niską jakość świadczonych usług telekomunikacyjnych,
- wysoką cenę tych usług, co sprawia, że wielu obywateli nie może z nich korzystać,
- niewielki dostęp do infrastruktury umożliwiającej komunikację bezprzewodową[109].

Charakteryzując poziom zaawansowania rewolucji informatycznej w Kirgistanie, można również przytoczyć raport Międzynarodowego Związku Telekomunikacyjnego *Measuring the Information Society* z 2010 roku. W ramach *ICT Development Index* kraj ten zajął dopiero 99. miejsce, wyprzedzając Algierię i Boliwię, natomiast w *ICT Price Basket* dopiero 125. miejsce (*Measuring the Information Society*, 2010: 2, 7). Widać więc wyraźnie, iż państwo to nie mogło posiadać zaawansowanych zdolności do odparcia poważnych cyberataków, implikowało to jednak zarazem stosunkowo niski stopień uzależnienia od technologii informacyjnych i komunikacyjnych, czyli teoretycznie mniejsze zagrożenie dla infrastruktury krytycznej.

[108] *Kyrgyzstan*. EU-Eastern Europe and Central Asia Gateway to ICT Research, Development and Policy Dialogue: www.eeca-ict.eu/countries/kyrgyzstan; dostep: 10.01.2014.

[109] T. Mambetalieva, Z. Shramko: *Kyrgyzstan*. Civil Initiative on Internet Policy, 2008: http://giswatch.org/sites/default/files/Kyrgyzstan_0.pdf; dostęp: 10.01.2014.

W styczniu 2009 roku, w apogeum debaty na temat amerykańskiej obecności wojskowej w Kirgistanie, doszło do szeregu poważnych cyberataków. Niespodziewanie 18 stycznia dwa główne przedsiębiorstwa udostępniające usługi internetowe (www.domain.kg, www.ns.kg) zostały zablokowane za pomocą metody *Distributed Denial of Service*. W efekcie wiele stron internetowych oraz usługi poczty elektronicznej stały się niedostępne dla użytkowników. Zdaniem Williama C. Ashmore'a (2009: 13) atak miał nastąpić tego samego dnia, w którym dyplomacja rosyjska rozpoczęła działania na rzecz usunięcia sił USA z lotniska wojskowego Manas. Analizę tych incydentów podjęła amerykańska korporacja SecureWorks Inc., która ustaliła, że miały one bardzo dużą skalę, ponieważ obaj dostawcy usług internetowych byli odpowiedzialni za funkcjonowanie ok. 80% krajowej sieci[110]. Z kolei według innych danych zaatakowane zostały aż trzy z czterech przedsiębiorstw udostępniających usługi internetowe, w tym m.in. AI ASIAINFO Autonomous System Bishkek. Co więcej, sparaliżowana miała zostać również usługa rejestracji domen internetowych. W tym kontekście pojawiły się wręcz głosy wskazujące na fakt, iż Rosja tworzyła w ten sposób swoistą „cyber-żelazną kurtynę", mającą oddzielać i kontrolować sieci komputerowe na obszarze byłych republik radzieckich[111]. Warto dodać, iż do cyberataków wykorzystano komputery znajdujące się na terytorium Federacji Rosyjskiej, co potwierdziła analiza adresów IP przeprowadzona przez Jeffreya Carra. Dodatkowo zauważył on, że serwery, z których kontrolowano tę operację, znajdowały się w Sankt Petersburgu (sieć AS) lub Moskwie (komputery Comcor TV). Oprócz adresów rosyjskich wykryto także udział jednostek znajdujących się w stolicy Arabii Saudyjskiej. Znajdowały się one na czarnej liście organizacji zwalczających spam w Internecie (Carr, 2012: 136—137).

Warto jednak zauważyć, iż w przeciwieństwie do *casusu* Estonii lub Gruzji w tym przypadku nie pojawiły się żadne ogólnodostępne dane dotyczące dokładnego zasięgu, przebiegu oraz skutków tych ataków. Zebrania wszystkich podstawowych informacji podjęła się wyspecjalizowana firma analityczna Arbor Networks. Jej ekspert Jose Nazario ze zdziwieniem odnotował na początku lutego 2009 roku, iż uzyskanie sprecyzowanych wiadomości na temat technicznych właściwości tych incydentów okazało się niezwykle trudne. Jedyną w zasadzie informacją, którą udało im się uzyskać, były pozostałości po DDoS (*ping flood*) z 28 stycznia 2009 roku[112]. Ta nietypowa sytuacja sprawiła, iż powstało

[110] C. Rhoads: *Kyrgyzstan Knocked Offline*. „The Wall Street Journal", 28.01.2009: http://online.wsj.com/news/articles/SB123310906904622741; dostęp: 10.01.2014; D. Jackson: *Kyrgyzstan Under DDoS Attack From Russia*. SecureWorks Research Blog, 27.01.2009: www.secureworks.com/resources/blog/research/research-20957; dostęp: 10.01.2014.

[111] J. Armin: *Cyberwar — The Cyber Iron Curtain: Now Kyrgyzstan — Part 1*. Host Exploit, 26.01.2009: www.hostexploit.com/index.php?option=com_content&view=article&id=96:cyberwar-the-cyber-iron-curtain-now-kyrgyzstan-part-1-&catid=1:articles; dostęp: 10.01.2014.

[112] J. Nazario: *Kyrgyzstan DDoS Attacks*. Arbor Networks, 02.02.2009: www.arbornetworks.com/asert/2009/02/kyrgyzstan-ddos-attacks; dostęp: 10.01.2014.

wiele koncepcji wyjaśniających rzeczywiste motywy sprawców. Warto więc przytoczyć kilka z nich.

Na wstępie można odwołać się do analizy Dona Jacksona z SecureWorks, który jako jeden z pierwszych podał szereg ciekawych informacji na temat tych incydentów. Oba ataki na ISP (*Internet Service Providers*) miały niemal identyczne cechy jak te z sierpnia 2008 roku. Ich głównym efektem było zablokowanie większości ruchu internetowego w kraju, który musiał zostać obsłużony przez inne, posiadające zdecydowanie mniejsze zdolności przedsiębiorstwa telekomunikacyjne. Ponadto Jackson podkreślił, iż ataki zostały przeprowadzone z rosyjskich komputerów, na co wskazywała wspomniana już analiza adresów IP. Powiązał je także z działalnością „rosyjskich cybermilicji", które miały w ten sposób wywrzeć nacisk na władze w Kirgistanie, aby rozwiązać kwestię bazy zgodnie z interesami Federacji Rosyjskiej. Chodziło tutaj nie tyle o prorosyjskie władze, lecz opozycję sprzeciwiającą się wyjściu Amerykanów. Według analityka „zdławienie poglądów ruchów opozycyjnych, w szczególności ich zdolności do prezentowania swojego stanowiska całemu światu za pomocą Internetu, z pewnością ma sens dla Rosji", zwłaszcza, iż tylko ona miała interes, aby przejąć pełną kontrolę nad „potęgą powietrzną" na „swoim własnym podwórku". Co za tym idzie, „atak DDoS byłby jedynym sposobem, aby powstrzymać opozycję od opublikowania alternatywnej [propozycji — M.L.] oraz zdobycia dla niej poparcia"[113]. W innej z wypowiedzi Don Jackson powiązał te incydenty z aktywnością wymienionej wcześniej Russian Business Network, twierdząc, iż większość pakietów danych przepływała przez kontrolowane przez nią sieci. Zdając sobie sprawę z powiązań RBN z rządem rosyjskim, doszedł więc do wniosku, iż za incydentami stał Kreml. Zresztą nawet inni, sceptyczni wobec tej teorii analitycy, zgodzili się, iż Rosja, nie podejmując kroków zapobiegawczych, niejako dała przyzwolenie na atak[114]. W tym kontekście warto ponownie odwołać się do słów Williama C. Ashmore'a (2009: 14), który zauważył, iż wydarzenia w Kirgistanie miały dwie cechy upodabniające je do przypadków Estonii i Gruzji: po pierwsze incydenty wynikały ze sprzeciwu wobec interesów rosyjskiego rządu, po drugie natomiast brak było dowodów, iż to Moskwa była w nie bezpośrednio zaangażowana.

Na odpowiedzialność Rosjan wskazywał również portal Strategy Page, który określił strategię Rosji z lat 2007—2009 mianem „cyberzastraszania". Tym razem jednak zdaniem jego ekspertów powodem nie były bynajmniej kwestie związane z bazą wojskową w Manas, lecz z próbami przejęcia kontroli nad kirgiskimi złożami ropy i gazu ziemnego. Dokonując ataków komputerowych,

[113] D. Jackson: *Kyrgyzstan Under DDoS Attack From Russia*. SecureWorks Research Blog, 27.01.2009: www.secureworks.com/resources/blog/research/research-20957; dostęp: 10.01.2014.

[114] D. Bradbury: *The fog of cyberwar*. „The Guardian" 05.02.2009: www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access; dostęp: 10.01.2014.

Moskwa miała zastosować wcześniej sprawdzoną taktykę i wymusić na prezydencie Bakiewie korzystne dla siebie porozumienie gospodarcze[115].

Zupełnie odmienną interpretację incydentów ze stycznia 2009 roku zaprezentował natomiast wspomniany Jeffrey Carr. Jego zdaniem nie miały one bezpośredniego związku z władzami Federacji Rosyjskiej, natomiast zdecydowanie więcej z samą sytuacją wewnętrzną w Kirgistanie. Podał on trzy grupy powodów. Przede wszystkim cyberataki zbiegły się w czasie z kryzysem politycznym, w którym partie opozycyjne zażądały ustąpienia prezydenta Bakiewa. W reakcji na te działania władze rozpoczęły represje. Ponadto zdaniem Carra podobne wydarzenia miały miejsce w 2005 roku, kiedy Bakiew doszedł do władzy: również wtedy doszło do cyberataków wymierzonych w jego politycznych przeciwników. Według analityka rząd Kirgistanu miał ponadto możliwość przeciwdziałania tym zagrożeniom, nie podjął jednak w tym względzie żadnych starań[116]. Taką interpretację poparło kilku innych badaczy, którzy wskazywali na fakt, iż władze w Biszkeku były same w sobie bardzo prorosyjskie, przez co dodatkowe środki nacisku nie miałyby sensu (Nazario, 2009: 163—181). Takiego scenariusza nie wykluczał też Rafał Rohozinski z OpenNet Initiative, który przyznał, że to sam Biszkek mógł wynająć rosyjskich hakerów: „Chodzi tu bardziej o uciszanie wewnętrznych dysydentów oraz wyeliminowanie jednego z głównych kanałów komunikacji grup opozycyjnych, jakim jest Internet"[117].

Wszystkie zaprezentowane powyżej teorie w ciekawy sposób podsumowali badacze z kanadyjskiego „Information Warfare Monitor". Ich zdaniem nie pojawiły się żadne dowody, które jednoznacznie przesądzałyby o tym, kto był rzeczywistym organizatorem ataków DDoS w Kirgistanie. Za bezpośrednich odpowiedzialnych uznano z kolei z dużą dozą prawdopodobieństwa osoby z rosyjskiego środowiska hakerów. Zauważono przy tym, iż zarówno rosyjski, jak i kirgiski rząd nie zareagowały natychmiastowo na te wydarzenia. Zdaniem „Information Warfare Monitor" Ministerstwo Spraw Wewnętrznych oraz Ministerstwo Komunikacji Federacji Rosyjskiej nie podjęły żadnych działań, których celem byłoby odcięcie sprawców od serwerów kontrolujących sieć *botnet*[118].

Reasumując powyższe rozważania, należy stwierdzić, iż w odróżnieniu od przypadków Estonii oraz Gruzji precyzyjna charakterystyka incydentów ze stycznia 2009 roku nie jest do końca możliwa. Wynika to z faktu, iż nawet wyspecjali-

---

[115] *Information Warfare: CyberBully*. Strategy Page, 01.02.2009: www.strategypage.com/htmw/htiw/articles/20090201.aspx; dostęp: 10.01.2014.

[116] R. Mackey: *Are 'Cyber-Militias' Attacking Kyrgyzstan?* „The New York Times" 05.02.2009: http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?_r=0; dostęp: 10.01.2014.

[117] D. Bradbury: *The fog of cyberwar…*, op.cit.

[118] *The Kyrgyzstan DDoS Attacks of January, 2009: Assessment and Analysis*. „Information Warfare Monitor" 28.01.2009: www.infowar-monitor.net/2009/01/the-kyrgyzstan-ddos-attacks-of-january-2009-assessment-and-analysis; dostęp: 10.01.2014.

zowane ośrodki badawcze nie były w stanie zebrać wystarczającej ilości danych, aby nie tylko odpowiedzieć na pytanie, kto był za nie odpowiedzialny, ale nawet aby prześledzić ich dokładny przebieg, skalę oraz skutki. Brakuje zatem podstawowych informacji mogących pomóc w interpretacji politycznych reperkusji tych wydarzeń. Niemniej opierając się na przytoczonych wyżej analizach można pokusić się o pewne ograniczone wnioski. Przede wszystkim nie ma wiarygodnych dowodów wskazujących, iż cyberataki wiązały się z chęcią przejęcia przez Rosję kontroli nad złożami surowców energetycznych w Kirgistanie. Wydarzenia te można więc interpretować w dwojaki sposób: albo jako konsekwencję rozgrywki międzynarodowej wokół bazy w Manas, albo też jako skutek rywalizacji na krajowej scenie politycznej. W obu przypadkach, jak wskazali zachodni eksperci, prawdopodobnie za paraliżem kirgiskiej sieci stały osoby związane z rosyjskim światkiem cyberprzestępczym. Ponadto nie wywołały one reakcji służb Federacji, które w żaden sposób nie starały się zablokować cyberataków ani też nie ukarały ich sprawców. Po raz kolejny zatem widoczne było pewne przyzwolenie Moskwy na szkodliwe dla innych państw działania w przestrzeni teleinformatycznej, co mogło wynikać z faktu, iż Kreml czerpał z nich znaczne korzyści polityczne. Jeśli celem rzeczywiście było wywarcie dodatkowego nacisku na rząd w Biszkeku, to na krótki czas udało się to osiągnąć. Jeśli zaś chodziło o stłumienie protestów opozycji, również leżało to w interesie Moskwy, obalenie prorosyjskiego prezydenta Bakiewa mogło bowiem skutkować zwrotem Kirgistanu w kierunku Stanów Zjednoczonych. Mimo to wbrew niektórym głosom trudno uznać te wydarzenia za dowód potwierdzający zjawisko rywalizacji państw w cyberprzestrzeni.

4.5. Operacja *Orchard*

Jak słusznie stwierdził Marcin Andrzej Piotrowski (2013: 6) z Polskiego Instytutu Spraw Międzynarodowych

> niezależnie od wydarzeń arabskiej wiosny 2011 roku Bliski Wschód znajduje się stale w centrum zainteresowania społeczności międzynarodowej, przede wszystkim ze względu na liczne konflikty wewnętrzne oraz międzypaństwowe. Zmiany kolejnych arabskich reżimów mogą ukształtować nowe relacje między nimi oraz modyfikować strategiczną mapę regionu. Kraje Afryki Północnej i Zatoki Perskiej oraz Izrael nie mają jednak wielostronnej architektury bezpieczeństwa regionalnego, która regulowałaby między nimi kwestie kontroli zbrojeń i rozbrojenia. Stan ten utrzymuje się pomimo upływu dwóch dekad od końca supermocarstwowej rywalizacji USA z ZSRR […]. Większość z kra-

> jów regionu jest co prawda sygnatariuszami porozumień globalnych (NPT, CTBT, BWC i CWC), ale nie przeszkodziło im to w rozwijaniu swoich programów broni masowego rażenia oraz środków ich przenoszenia. Wiele z nich postrzega swoich sąsiadów jako wrogów lub kwestionuje granice wytyczone po 1945 roku.

Podobne stanowisko zajęła Katarzyna Czornik (2012: 11), której zdaniem

> arabski nacjonalizm, panarabizm, liczne podziały, antagonizmy i konflikty wewnątrzregionalne, spory dynastyczne i narodowościowe, rozbieżności interesów politycznych, gospodarczych, ideologicznych i terytorialnych, nieuregulowane kwestie demarkacji granic, rywalizacja o miano *primus inter pares* w regionie, a także podziały religijne i etniczne przez wieki determinowały sytuację geopolityczną Bliskiego Wschodu, implikując zainteresowanie i zaangażowanie państw w tej części świata.

Ze względu na niekorzystne położenie geopolityczne, które wymuszało wysoką skuteczność podejmowanych inicjatyw na arenie międzynarodowej, po II wojnie światowej wyjątkową rolę w tym niezwykle skomplikowanym i groźnym środowisku odgrywał bez wątpienia Izrael. Umiejętnie stosując różnorodne i często nowatorskie metody przeciwdziałania niekorzystnym dla siebie procesom i tendencjom, był on w większości przypadków w stanie zapewnić bezpieczeństwo swoim obywatelom (Dowty, 1999). Jednym z symboli takiego podejścia było z pewnością zbombardowanie przez IDF irackiego reaktora atomowego w Osiraku w czerwcu 1981 roku w ramach operacji *Opera* (Raas, Long, 2007: 7—33). W tendencje te z czasem zaczęło się wpisywać również wykorzystanie najnowszych technologii teleinformatycznych, których znaczenie stosunkowo szybko zostało dostrzeżone przez Tel Awiw. W związku z tym władze wsparły zarówno procesy kształcenia wysokiej klasy specjalistów z zakresu ICT, jak i przeznaczyły znaczne środki finansowe na rozwój tego sektora gospodarki, szczególnie jeśli chodzi o innowacyjne badania naukowe (Dutta, Lopez-Claros, Mia, 2006: 89—104). Pozwoliło to na szybkie osiągnięcie znaczącej przewagi nad innymi krajami regionu, a co za tym idzie na uzyskanie dodatkowych możliwości związanych z wykorzystaniem cyberprzestrzeni jako nowego wymiaru oddziaływania na środowisko międzynarodowe. Dotychczas opinia publiczna dowiedziała się o dwóch przypadkach, w których cyberataki stały się swoistym instrumentem polityki zagranicznej Izraela. Chronologicznie pierwszym z nich była izraelska operacja zbrojna przeciwko Syrii o kryptonimie *Orchard*, przeprowadzona we wrześniu 2007 roku, którą warto scharakteryzować nieco szerzej.

Na wstępie należałoby zauważyć, iż relacje izraelsko-syryjskie od zarania miały niezwykle burzliwy charakter. Już w listopadzie 1947 roku Syria sprzeciwiła się planom Zgromadzenia Ogólnego ONZ, które zaproponowało

stworzenie sąsiadującego z krajami arabskimi państwa żydowskiego. Doprowadziło to do inwazji na Izrael w maju 1948 roku, która zakończyła się jednak porażką Arabów i zawieszeniem broni w lipcu 1949 roku. Ze względu na oczywisty brak rekoncyliacji w kolejnych latach wrogość na linii Tel Awiw — Damaszek utrzymywała się nadal na wysokim poziomie. Symbolicznym wyrazem tego stanu rzeczy stała się wojna w 1967 roku. W jej wyniku Syria utraciła na rzecz Izraela strategicznie położone Wzgórza Golan[119]. Warto również wspomnieć o wojnie Yom Kippur, podczas której Syria wraz z sojusznikami podjęła nieudaną próbę ich odzyskania. Nie zakończyło to oczywiście okresu napięć i konfliktów w relacjach dwustronnych, co wpisywało się w szerszą logikę stosunków na linii Izrael — państwa arabskie. Do kolejnych starć zbrojnych między nimi doszło w roku 1974 na Wzgórzach Golan oraz w 1982 roku w Libanie. W obu przypadkach to Damaszek poniósł porażkę. W kolejnych dekadach między oboma państwami, znajdującymi się zresztą formalnie w stanie wojny, mimo pewnych nieudanych prób porozumienia (w latach 1995—1996 i 1999—2000) nadal dochodziło do poważnych incydentów zbrojnych[120].

Z perspektywy syryjskiej w ciekawy sposób główne cechy relacji z Izraelem opisał Paul Salem (2008: 2). Zauważył on, iż jednym z kluczowych celów polityki zagranicznej Syrii było odzyskanie Wzgórz Golan. Wynikało to w dużej mierze z faktu, iż w 1967 roku Hafez al Assad był ministrem obrony narodowej. Utrata tego obszaru była traktowana jako swoista „plama na honorze" reżimu i rodziny. Porażka w 1973 roku zmusiła Damaszek do rywalizowania z Izraelem w sposób niebezpośredni, polegający głównie na wspieraniu Organizacji Wyzwolenia Palestyny, a po 1982 roku Hezbollahu. Zdaniem analityka Carnegie Endowment for International Peace po dojściu do władzy Baszara al Assada strategia ta była kontynuowana. Z jednej strony Damaszek wywierał nacisk na Izrael za pomocą tzw. *proxies*, w tym głównie Hezbollahu, z drugiej natomiast dążył do wznowienia negocjacji dwustronnych (Salem, 2008: 2). Polityka nowego przywódcy w dużej mierze okazała się jednak nieefektywna, czego wyrazem było osłabienie geopolitycznej pozycji Syrii na Bliskim Wschodzie. Złożyło się na to szereg wydarzeń. Przede wszystkim wpływ na to miała aktywność Stanów Zjednoczonych po 11 września 2001 roku. Jak wskazał Raymond Hinnebusch, zamachy terrorystyczne na World Trade Center dały USA możliwość uznania tradycyjnych wrogów Izraela za własnych przeciwników, dwuznaczne stanowisko Syrii wobec „wojny z terroryzmem" dopro-

[119] Szerzej: Jawasreh, 2003: 285—286; Pogońska-Pol, 2012: 299—311; *Timeline: A chronology of Israel — Syria relations since 1947*. „Haaretz" 06.09.2007: www.haaretz.com/news/timeline-a-chronology-of-israel-syria-relations-since-1947-1.228952; dostęp: 17.01.2014; Zając, 2009: 184; Dajani, 2011.

[120] Jawasreh, 2003: 285—286; *Timeline: A chronology of Israel-Syria relations since 1947*…, op.cit.

wadziło więc do ochłodzenia stosunków bilateralnych, Damaszek wspierał bowiem wywiadowczo amerykańskie wysiłki na rzecz zwalczania Al Kaidy, zarazem nie godząc się na zerwanie współpracy z Hezbollahem[121]. Kolejnym czynnikiem, który doprowadził do zachwiania pozycji Syrii, była również amerykańska inwazja na Irak w 2003 roku. Co prawda al Assad pozostał raczej na uboczu ówczesnych wydarzeń, sprzeciwiał się jednak interwencji zbrojnej, która oznaczała m.in. wzmocnienie pozycji Izraela (Czornik, 2012: 334), a także zbliżenie sił amerykańskich do granic oraz utrudnienie współpracy z Iranem[122]. Po trzecie w tym czasie do władzy w Izraelu doszedł Ariel Szaron, polityk, który nie widział możliwości prowadzenia negocjacji z reżimem w Damaszku (*Restarting Israeli-Syrian Negotiations*, 2007: 2). Po czwarte w połowie pierwszej dekady XXI wieku doszło do znacznego osłabienia pozycji Syrii w Libanie, postrzeganym jako państwo o strategicznym znaczeniu dla jej wpływów w regionie. W efekcie została ona zmuszona do wycofania swoich sił z tego kraju w 2006 roku (Lizak, 2007: 223). W tym samym roku doszło ponadto do dalszego osłabienia jej pozycji międzynarodowej, co było skutkiem wojny w Libanie (Salem, 2008: 2). Ponadto, jak podkreślił Elliot M. Repko (2007: 28), przedłużający się okres okupacji Wzgórz Golan przez Tel Awiw sprawiał, że jego powrót w granice Syrii stawał się coraz bardziej utrudniony.

W świetle tych niekorzystnych tendencji Syria stała się na początku XXI wieku państwem w dużej mierze izolowanym na arenie regionalnej i światowej, zniechęcając do siebie m.in. część partnerów arabskich, głównym efektem tych procesów było więc uzależnienie Damaszku od współpracy z reżimem ajatollahów (Dzisiów-Szuszczykiewicz, 2012: 92—93). Zdaniem Paula Salema (2008: 2) dość znamienne było jednak, że Teheran nie posiadał wystarczającego potencjału, aby skutecznie pomóc Syrii w stosunkach z Izraelem, co implikowało potrzebę poszukiwania innych środków, które pozwoliłyby zapewnić niezbędny poziom bezpieczeństwa narodowego oraz wzmocnić pozycję al Assada w rozgrywce z Tel Awiwem oraz Waszyngtonem. W sytuacji, w której jego uprzywilejowany status w Libanie został przekreślony, stosunki z innymi państwami arabskimi nadwyrężone, a sama Syria znalazła się w geopolitycznych kleszczach między Izraelem a kontrolowanym przez USA Irakiem, władze w Damaszku uznały, że najbardziej oczywistym i korzystnym rozwiązaniem miał być rozwój broni masowego rażenia. Syria dysponowała już dużymi zasobami broni chemicznej oraz bogatymi środkami jej przenoszenia, w tym setkami rakiet bali-

[121] R. Hinnebusch: *Defying the Hegemon: Syria and the Iraq War*. European Consortium on Political Research Conference, Budapest, September 2005, s. 5: www.st-andrews.ac.uk/media/school-of-international-relations/mecacs/workingpapers/defying_the_hegemon.pdf; dostęp: 17.01.2014.

[122] R. Hinnebusch: *Defying the Hegemon*…, op.cit., s. 5—7.

stycznych[123], bombowcami[124] oraz artylerią. Arsenał ten nie gwarantował jednak pełnego bezpieczeństwa, czego dowodziły zresztą kolejne incydenty zbrojne z Izraelem. W związku z tym reżim al Assada doszedł do wniosku, iż najskuteczniejszym środkiem zabezpieczenia państwa oraz wzmocnienia jego pozycji w regionie będzie uzyskanie broni atomowej[125]. Było to tym wyraźniejsze, iż prace nad rozwojem technologii nuklearnych od dawna prowadził jego najbliższy sojusznik — Teheran. Oczywiście program ten musiał być ściśle tajny, gdyż od 1968 roku Syria była sygnatariuszem traktatu NPT oraz obawiała się ewentualnej reakcji zbrojnej ze strony Izraela.

Syryjskie próby rozwoju technologii tego typu miały długą historię. Już w latach 80. XX wieku Damaszek nawiązał cywilną współpracę w tej dziedzinie z Argentyną, Chińską Republiką Ludową oraz Rosją, wysiłki te przez lata nie przynosiły jednak oczekiwanych rezultatów. Dopiero w grudniu 1991 roku chińscy technicy rozpoczęli budowę pierwszego naukowego reaktora atomowego SRR-1 w Der al Hadjar. Zaczął on działać w 1996 roku i znajdował się pod pełną kontrolą Międzynarodowej Agencji Energii Atomowej (Cordesman, Nerguizian, Popescu, 2008: 212). Na tym tle próbę rozpoczęcia wojskowego programu atomowego podjęto dopiero na początku XXI wieku. Oprócz omówionych wyżej kwestii w dużym stopniu przyczyniły się do tego trzy wydarzenia. Po pierwsze w 2001 roku nawiązano współpracę z Koreą Północną, której celem była budowa w Syrii reaktora zdolnego produkować pluton. Został on zlokalizowany w odosobnieniu, na pustyni w regionie Deir ez Zor. Po drugie według części doniesień po interwencji amerykańskiej w Iraku w 2003 roku iraccy specjaliści ds. technologii nuklearnych uciekli właśnie do Damaszku, gdzie wsparli prace nad reaktorem. Po trzecie zgodnie z informacjami ujawnionymi przez amerykański wywiad w 2006 roku syryjskie władze nawiązały kontakt z siatką Abdula Qadeera Khana, odpowiedzialnego za sprzedaż technologii nuklearnych m.in. do Libii i Iranu (Ibidem, s. 212—213).

Stosunki dwustronne nieco inaczej wyglądały natomiast z perspektywy Tel Awiwu, który działania Syrii postrzegał jako egzystencjalne zagrożenie. Ideologia arabskiego nacjonalizmu, która była rozpowszechniona w tym kraju, była uznawana w Izraelu za z gruntu antysemicką. Potwierdzały to zresztą kolejne akcje Damaszku, zmierzającego konsekwentnie do osłabienia jego bezpieczeństwa. W tym kontekście objęcie władzy przez Baszara al Assada w zasadzie nie

[123] *Syria Overview*. NTI: www.nti.org/country-profiles/syria; dostęp: 18.01.2014; *Worldwide Ballistic Missile Inventories*. Arms Control Association, January 2012: www.armscontrol.org/factsheets/missiles; dostęp: 18.01.2014.

[124] Cordesman, 2008; L. Stoker: *Aircraft of the Syrian Air Force: from Russia. with weaponry*, Airforce Technology, 25.06.2012: www.airforce-technology.com/features/featurerussia--with-weaponry-syrias-air-force; dostęp: 18.01.2014.

[125] *Syria*. Nuclear Files: http://nuclearfiles.org/menu/key-issues/nuclear-weapons/issues/proliferation/syria/index.htm; dostęp: 18.01.2014.

zmieniło optyki stosunków bilateralnych ze strony Izraelczyków, którzy upatrywali w nim wroga, przeciwdziałającego ich interesom m.in. w Libanie. Na tym kierunku do głównych wyzwań zaliczano naturalnie jego pogłębioną współpracę z Iranem oraz Hezbollahem. Z jednej strony rząd Ariela Szarona wskazywał na pełną odpowiedzialność Damaszku za kolejne incydenty wywołane przez Hezbollah (Rabinovich, 2012: 1—3), z drugiej kooperacja z Teheranem była szczególnie kłopotliwa po 2002 roku, kiedy ujawniono program atomowy reżimu ajatollahów (zob. Piotrowski, 2012: 31—72; Simon, 2009).

Stosunki z Syrią wpisywały się zarazem w szerszą logikę całokształtu polityki zagranicznej Izraela, której główną przesłanką było oczywiście zwalczanie egzystencjalnych zagrożeń dla swojego bezpieczeństwa. Jim Zanotti (2013: 13) wyodrębnił trzy filary, na których Tel Awiw tradycyjnie opierał swoją politykę bezpieczeństwa: miażdżącą przewagę w uzbrojeniu konwencjonalnym, wyłączność (choć nieoficjalną) na broń atomową w regionie oraz porozumienia *de iure* lub *de facto* z przywódcami arabskich reżimów autorytarnych, zmierzające do zapobieżenia konfliktom międzypaństwowym (Zanotti, 2013: 13).

Wszystkie części składowe polityki bezpieczeństwa Izraela na Bliskim Wschodzie oparte zostały jednak przede wszystkim na strategicznej współpracy ze Stanami Zjednoczonymi. Jak zauważyła Katarzyna Czornik (2011: 92—93), zarówno w czasie zimnej wojny, jak i po jej zakończeniu pozostawał on niekwestionowanym sojusznikiem USA w regionie. Uznając go za cennego i silnego partnera, położonego wśród wrogich reżimów arabskich, administracja amerykańska tradycyjnie dokładała starań, aby zapewnić Tel Awiwowi bezpieczeństwo, a także podkreślić jego prawa do istnienia oraz samoobrony. Najbardziej dobitnym wyrazem partnerstwa obu państw była wielowymiarowa pomoc amerykańska dla Izraela, której wartość w latach 1949—2007 ocenia się na zawrotną sumę ponad 101 mld dolarów, z czego wartość pomocy wojskowej oscylowała w granicach ok. 53 mld dolarów. Podobne zdanie wyraziła Joanna Dyduch (2011: 357—358), według której

> rolę najważniejszego sojusznika Izraela na arenie międzynarodowej przypisuje się Stanom Zjednoczonym. Stąd USA jest postrzegane jako ważny filar bezpieczeństwa Izraela […]. Nieco upraszczając, wydaje się, że istnieją dwie podstawowe determinanty zaangażowania USA na rzecz Izraela. Pierwsza ma związek ze strategicznym położeniem Izraela w istotnym z punktu widzenia politycznych i ekonomicznych interesów amerykańskich w tym regionie świata. Druga — o ogromnym znaczeniu w procesie formułowania celów amerykańskiej polityki zagranicznej — to obecność wpływowego proizraelskiego (głównie żydowskiego) lobby w Stanach Zjednoczonych.

W tym kontekście współpraca na linii Tel Awiw — Waszyngton w zasadniczym stopniu umacniała pozycję Izraela na Bliskim Wschodzie.

W tej perspektywie pewna zmiana w polityce Izraela wobec Syrii nastąpiła w okresie rządów Ehuda Olmerta. Jednym z wydarzeń, które na to wpłynęło, była wojna w Libanie w 2006 roku. Brak wyraźnego sukcesu armii izraelskiej w konflikcie z Hezbollahem (Nakhleh, 2007) zdaniem Itamara Rabinovicha udowodnił, jak dużym zagrożeniem jest współpraca tej organizacji z Damaszkiem i Teheranem[126]. Tym bardziej, iż, jak wskazywał Wiesław Lizak (2007: 224)

> ze względu na związki Hizb'ullahu z Syrią i Iranem pojawiło się wiele komentarzy wskazujących na Damaszek i/lub Teheran jako możliwe źródło inspiracji dla konfliktu. Wskazywano m.in. na chęć odwrócenia uwagi od irańskiego programu atomowego bądź też syryjskiego zaangażowania w zabójstwo Rafika al-Haririego jako potencjalne przyczyny podsycania konfliktu z Izraelem.

Jednak wbrew nadziejom m.in. Stanów Zjednoczonych premier Izraela tym razem nie był skłonny odwołać się do środków militarnych. Wręcz przeciwnie: zwrócił się ponownie ku instrumentom dyplomatycznym, inicjując negocjacje z reżimem Baszara al Assada[127]. Ich wykorzystanie zakończyło się jednak szybko fiaskiem ze względu na operację izraelską w Strefie Gazy. Al Assad w jej wyniku wycofał się z rozmów, nawołując przy tym inne państwa arabskie do zerwania wszelkich stosunków z Tel Awiwem (Migdalovitz, 2010: 40—42).

Drugim wydarzeniem, które przyczyniło się do zmian w stosunkach dwustronnych, było odkrycie przez wywiad izraelski syryjskiego programu atomowego. Izrael wprawdzie już od 2001 roku posiadał pewne informacje wskazujące na atomowy kontekst współpracy z KRLD, jednak według doniesień mediów Mossad miał odrzucić tego typu sugestie wywiadu wojskowego. Niedługo później, w 2003 roku, amerykańska Agencja Bezpieczeństwa Narodowego (National Security Agency) zwróciła uwagę na wyjątkowo dużą liczbę połączeń telefonicznych między Phenianem a miejscowością Al Kibar na syryjskiej pustyni. Informację tę przekazano izraelskiej jednostce wywiadu elektronicznego nr 8200, która zaczęła aktywnie śledzić ten obszar[128]. Był to więc pierwszy moment, kiedy technologie teleinformatyczne odegrały znaczącą rolę w tych wydarzeniach. Do odkrycia syryjskiego programu atomowego doszło jednak zdecydowanie później, dopiero w 2006 roku. W wysiłkach tych fundamentalną rolę odegrały ponownie ICT. Jeden z przedstawicieli syryjskiego rządu odbył wówczas podróż do Londynu, gdzie zameldował się w jednym z luksusowych

[126] Rabinovich, 2012, s. 3; B. Ravid, A. Harel, A. Issacharoff: *Olmert labels Syria talks 'historic breakthrough'*. „Haaretz", 22.05.2008: www.haaretz.com/print-edition/news/olmert-labels-syria-talks-historic-breakthrough-1.246321; dostęp: 17.01.2014.

[127] Rabinovich, 2012, s. 3; B. Ravid, A. Harel, A. Issacharoff, op.cit.

[128] N. Klieger: *A strike in the desert*. YNET News, 11.02.2009: www.ynetnews.com/articles/0,7340,L-3799227,00.html; dostęp: 18.01.2014.

hoteli w Kensington. Mossad, który śledził poczynania polityka, zdecydował się na próbę infiltracji, której celem było uzyskanie danych znajdujących się na jego prywatnym notebooku. Operacja w pełni się udała, polityk pozostawił bowiem komputer w pokoju hotelowym. W efekcie agenci zdołali zainstalować na nim złośliwy program typu trojan, dzięki któremu mogli uzyskać zdalny dostęp do wszystkich danych na twardym dysku. Odnaleźli tam m.in. plany konstrukcyjne reaktora, wiadomości poczty elektronicznej potwierdzające istnienie programu, a także setki zdjęć kompleksu atomowego w różnych stadiach budowy. Potwierdzono przy tym, iż celem tej konstrukcji była produkcja materiałów rozszczepialnych. Znaleziono również fotografie głowy północnokoreańskiego programu atomowego Chona Chibu oraz szefa Syryjskiej Komisji Energii Atomowej Ibrahima Othmana. Wszystkie te wiadomości zostały prawidłowo zinterpretowane i wywołały energiczną reakcję rządu Olmerta, który przed podjęciem ostatecznej decyzji zażądał jeszcze dodatkowych danych na temat kompleksu[129]. Dostarczył ich prawdopodobnie generał Gwardii Rewolucyjnej Ali Reza Asgari, który w 2007 roku uciekł z Iranu. Do przekonania władz do podjęcia działań przyczynił się również raport generała Yaakova Amirdora, który stwierdził jednoznacznie, iż program nuklearny stanowi egzystencjalne zagrożenie dla Izraela. Świadczyły o tym ponadto informacje zebrane przez Mossad na temat transportowanych z Korei Północnej materiałów i urządzeń. W rezultacie Ehud Olmert zgodził się na zrealizowanie operacji zbrojnej, której celem miało być zniszczenie syryjskiego reaktora jądrowego[130]. Zgodę na tę misję wyraziły również Stany Zjednoczone.

Operacja *Orchard* została przeprowadzona w nocy z 5 na 6 września 2007 roku przez 10 samolotów bojowych F-15 IDF. Wystartowały one z bazy w Ramat David i skierowały się nad Morze Śródziemne. Po pewnym czasie trzem z nich wydano rozkaz powrotu do bazy, podczas gdy pozostałe siedem kontynuowało lot w kierunku północno-wschodnim na niskim pułapie, po czym zniszczyło radar w Tall al Abuad, a następnie zbombardowało reaktor w Al Kibar. Po zrealizowaniu zadania samoloty nie niepokojone powróciły do Izraela[131]. Stosun-

[129] K. Zetter: *Mossad Hacked Syrian Offical's Computer Before Bombing Mysterious Facility*. „Wired", 11.03.2009: www.wired.com/threatlevel/2009/11/mossad-hack; dostęp: 18.01.2014; E. Follath, H. Stark: *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor*. Spiegel Online, 02.11.2009, s. 2: www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html; dostęp: 18.01.2014.

[130] E. Follath, H. Stark: *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor*. Spiegel Online, 02.11.2009, s. 3: www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html; dostęp: 18.01.2014.

[131] Cordesman, Nerguizian, Popescu, 2008, s. 213—214; D. Makovsky: *The silent strike*. „The New Yorker" 17.09.2012: www.newyorker.com/reporting/2012/09/17/120917fa_fact_makovsky; dostęp: 18.01.2014.

kowo szybko pojawiły się zasadne pytania, w jaki sposób samoloty bojowe IDF były w stanie przelecieć dwukrotnie nad Syrią, nie alarmując przy tym stosunkowo zaawansowanego systemu obrony przeciwlotniczej, o którego skuteczności świadczyły zresztą późniejsze wydarzenia z czerwca 2012 roku, kiedy Syryjczycy zestrzelili turecki samolot F-4, który naruszył wspólną granicę morską[132]. Na wątek ten zwróciło uwagę m.in. amerykańskie czasopismo specjalistyczne „Aviation Week" w wydaniu z listopada 2007 roku. W opublikowanym tam artykule przywołano informacje podane przez amerykańskich analityków związanych z wywiadem. Według nich aby siły zadaniowe izraelskiej armii nie zostały wykryte i zniszczone, nie tylko zbombardowano wspomniany radar, ale wręcz wyłączono na okres rajdu lotniczego cały system przeciwlotniczy Syrii. Cel ten zrealizowano w dwojaki sposób. Z jednej strony zastosowano tradycyjne metody walki elektronicznej, w tym zakłócania systemów radarowych, z drugiej zgodnie z sugestiami anonimowych przedstawicieli wywiadu USA pewną rolę odegrał tu atak komputerowy, który miał za zadanie nie tylko zablokować system obrony przeciwlotniczej, ale także, jak przyznali, zakłócić system dowodzenia i kontroli syryjskiej armii. Zastosowanie tego typu środków nie zostało co prawda bezpośrednio potwierdzone przez izraelskie władze, na prawdziwość tych informacji wskazywała jednak wypowiedź jednego z przedstawicieli Ministerstwa Obrony Pinchasa Buchrisa, który stwierdził: „Ofensywna i defensywna walka sieciowa jest jednym z najbardziej interesujących nowych obszarów […]. Mogę tylko powiedzieć, że przykładamy do [tej — M.L] technologii wielkie znaczenie. Wątpiłem w nią pięć lat temu […]. Teraz wszystko się zmieniło"[133].

Te stosunkowo ogólne informacje, które pojawiły się niedługo po operacji *Orchard*, przyciągnęły uwagę wielu specjalistów z zakresu bezpieczeństwa teleinformatycznego, którzy zaczęli zastanawiać się, jakimi środkami Izrael mógł osiągnąć tego typu efekt (Gupta, Joshi, 2012: 387), ponieważ w porównaniu z nimi cyberataki z Estonii z kwietnia 2007 roku wydawały się dosyć prymitywne. Można tu wskazać na kilka możliwych wyjaśnień. Sally Adee z magazynu „IEEE Spectrum" zasugerowała, iż czasowe sparaliżowanie elementów syryjskiego systemu obronnego mogło być rezultatem zastosowania tzw. *kill switch*. Część analityków była zdania, że syryjskie komputery wojskowe oraz inne urządzenia kontrolujące radary mogły wykorzystywać popularne, komercyjne procesory, w których możliwe było wbudowanie tzw. *backdoorów* pozwalających na zdalną i nieuprawnioną manipulację. Wysyłając specjalny kod,

[132] D. Cenciotti: *Air Strike on Damascus Military Complex Shows Syrian Air Defense Can Do Nothing Against Israeli Electronic Warfare*. „The Aviationist" 01.02.2013: http://theaviationist.com/tag/operation-orchard; dostęp: 18.01.2014.

[133] D.A. Fulgham, R. Wa: *U.S. Electronic Surveilance Monitored Israeli Attack On Syria*. World Security Network, 23.11.2007: www.worldsecuritynetwork.com/Israel-Palestine/David-A.-Fulghum-and-Robert-Wall-/U.S.-Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria; dostęp: 18.01.2014.

osoba uprawniona mogła zablokować dzięki temu każde urządzenie, w którym tego typu układy scalone zostały zainstalowane[134]. Jak zauważył John Marke, jest to globalnie coraz poważniejszy problem, gdyż wykrycie kilkuset tysięcy, a nawet milionów „podrobionych" tranzystorów na mikroczipach posiadających ich setki milionów jest niezwykle trudne[135]. W konsekwencji na zagrożenia te w ostatnich latach zaczęło zwracać uwagę coraz więcej rządów. Podjęły one działania zmierzające do zapewnienia, aby wszelkie urządzenia komputerowe stosowane na obszarach o strategicznym znaczeniu dla bezpieczeństwa państwa były wyprodukowane przez kontrolowane przez wywiad, rodzime przedsiębiorstwa[136].

Z kolei inni eksperci stwierdzili, iż możliwym wytłumaczeniem „oślepienia" systemu obrony przeciwlotniczej reżimu al Assada było zastosowanie zaawansowanego oprogramowania wojskowego produkcji BAE Systems o nazwie *Suter*. Głównym zadaniem tej aplikacji były ataki na systemy komputerowe oraz telekomunikacyjne potencjalnego przeciwnika, w tym w szczególności systemy obrony przeciwlotniczej. Zgodnie z informacjami podanymi przez Davida A. Fulghama, Michaela A. Dornheima oraz Williama B. Scotta stworzono trzy wersje tego programu. *Suter 1* miał pozwalać na sprawdzenie, co widzą systemy radarowe przeciwnika. *Suter 2* był bardziej zaawansowany, umożliwiał bowiem przejęcie kontroli nad systemami i sieciami wojskowymi z uprawnieniami administratora, co pozwalało na bezpośrednią manipulację sensorami. *Suter 3* miał pozwalać na uzyskanie dostępu do innych systemów o krytycznym znaczeniu dla wydarzeń na polu walki, w tym np. wyrzutni rakiet balistycznych[137]. Ciekawe informacje na temat funkcjonowania programu *Suter* podał Richard B. Gasperre ze specjalistycznego amerykańskiego portalu Airforce Technology. Według niego ten wojskowy trojan składał się z dwóch komponentów: jednego odpowiedzialnego za jego zainstalowanie we wrogich systemach teleinformatycznych oraz drugiego, który pozwalał monitorować wyniki jego funkcjonowania. Później dodano jeszcze trzeci, odpowiedzialny za kontrolę wrażliwych elementów wrogiego systemu obronnego. Co ciekawe, jego użycie oparte było w przypadku sił USAF na kilku rodzajach samolotów. Po pierwsze na RC-135

---

[134] S. Adee: *The Hunt for the Kill Switch*. „IEEE Spectrum" 01.05.2008: http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0; dostęp: 18.01.2014.

[135] J. Marke: *We Have Crossed Into Syrian Airspace, Operation Orchard. An Allegatory on Microchips, Espionage & Economic Warfare*. Prologue, 2010: http://jmarke.wordpress.com/2011/09/08/israel%E2%80%99s-operation-orchard-%E2%80%93-victory-on-a-microchip; dostęp: 19.01.2014.

[136] Zob. np. J. Villasenor: *Ensuring Hardware Cybersecurity*. „Issues of Technology Innovation" May 2011, nr 9: www.brookings.edu/research/papers/2011/05/hardware-cybersecurity; dostęp: 18.01.2014; *Cyber Defense Hardware Vulnerabilities*, 2011.

[137] D.A. Fulgham, M.A. Dornheim, W.B. Scott: *Black Surprises (USAF can take control of enemy missile launchers, radars, etc.)*. Aviation Now, January 2007: www.freerepublic.com/focus/f-news/1773240/posts; dostęp: 18.01.2014.

Rivet Joint przeznaczonych do prowadzenia wywiadu elektronicznego, które były odpowiedzialne za monitorowanie wyników działania programu *Suter*. Po drugie znaczną rolę odrywały EC-130 *Compass Call* przeznaczone do walki elektronicznej, w tym zakłócania systemów dowodzenia wroga. USAF mogło wykorzystywać samoloty F-16CJ, które stanowiły drugą linię wsparcia, w wypadku gdyby oprogramowanie zawiodło i nie sparaliżowało obrony przeciwlotniczej przeciwnika. Najbardziej interesujące informacje podane przez autora dotyczyły jednak specyfiki działania trojana. Otóż stwierdzono, iż do „zarażenia" wrogich systemów mogło dochodzić w sposób bezprzewodowy, właśnie przy pomocy samolotu EC-130. W odróżnieniu od tradycyjnych środków walki elektronicznej ich zablokowanie nie polegało na ich „zalaniu" nadmierną ilością sygnałów czy mocy, lecz wprowadzeniem wyspecjalizowanych algorytmów i komend do namierzonych komputerów wojskowych. Dzięki temu *Suter* mógł infekować wszystkie dostępne sieci, zarówno przewodowe, jak i bezprzewodowe. Jak zauważył Gasperre, jego operatorzy byli więc w stanie przejąć kontrolę nad wrogimi radarami, modyfikując m.in. pracę sensorów w ten sposób, aby nie wykryły one nadlatujących samolotów. Nawet jeśli administratorzy systemów obrony przeciwlotniczej wykryliby cyberatak, usunięcie jego skutków nie było rzeczą prostą[138].

Odnosząc te informacje do wydarzeń z 2007 roku, Richard B. Gasperre zauważył kilka istotnych kwestii. Po pierwsze według niego izraelskim odpowiednikiem wymienionych wyżej wyspecjalizowanych samolotów USAF były Gulfstream G550, Tel Awiw posiadał zatem techniczne możliwości użycia tego typu trojana. Po drugie w lecie 2007 roku Izrael wystrzelił satelitę szpiegowskiego *Ofek*-7, co pozwoliło mu uzyskać dokładne dane na temat rozkładu konstruowanego obiektu. Zdaniem autora głównym powodem takiego przebiegu wydarzeń była ponadto przestarzała architektura syryjskiego systemu obrony przeciwlotniczej, który był co prawda dość zaawansowany, lecz jednocześnie scentralizowany. Bez wykorzystania oprogramowania typu *firewall*[139] szansa na obronę przed trojanem była znikoma[140]. Na tym tle należy jednak podkreślić, że nigdy oficjalnie nie potwierdzono, iż programem użytym przez Izrael był rzeczywiście *Suter*. Być może, jak wskazują późniejsze poczynania Izraela w stosunkach z Iranem, wykorzystano inne narzędzia o podobnych właściwościach technicznych.

Wszystkie przytoczone wyżej informacje i teorie wskazywały więc jednoznacznie na fakt, iż Izrael, chcąc sparaliżować systemy obrony przeciwlotniczej przeciwnika, odwołał się do niezwykle zaawansowanego jak na te czasy cyber-

[138] R.B. Gasperre: *The Israeli „E-tack" on Syria — Part II.* Airforce Technology, 11.03.2008: www.airforce-technology.com/features/feature1669; dostęp: 19.01.2014.

[139] Inaczej zapora ogniowa, zapora internetowa. Może ona chronić całą sieć lub każdy z komputerów z osobna przed nieuprawnionym dostępem z zewnątrz. Zob. Kępa, 2014: 260.

[140] R.B. Gasperre: *The Israeli „E-tack" on Syria — Part II…*, op.cit.

ataku. Trudno bowiem oczekiwać, aby wykorzystane w operacji samoloty F-15 i F-16, nieposiadające właściwości *stealth*, bez zastosowania niekonwencjonalnych metod ataku nie zostały wykryte przez stosunkowo silną obronę przeciwlotniczą reżimu al Assada. Cyberatak polegał albo na wykorzystaniu wcześniej wbudowanych, wadliwych elementów sprzętu komputerowego wroga, albo też, co bardziej prawdopodobne, na zastosowaniu niezwykle zaawansowanego złośliwego programu. Niestety ze względu na charakter tej operacji, która wzięła na cel elementy infrastruktury wojskowej, sporządzenie analiz przez niezależne ośrodki badawcze okazało się w tym przypadku niemożliwe, a zatem sformułowanie ostatecznych wniosków w oparciu o obiektywne dane było niezwykle trudne. Niemniej ze względu na wszystkie wymienione wyżej kwestie wśród badaczy w dużej mierze panuje konsensus co do tego, że Izrael odwołał się w tym wypadku do działań w cyberprzestrzeni. Było to tym wyraźniejsze, iż od lat dynamicznie rozwijał on swój potencjał w tej dziedzinie. Warto tu przywołać opinię Freda Schreiera (2015: 111), który stwierdził, że

> jakkolwiek szczegóły operacji są niejasne, a formalne przypisanie odpowiedzialności [za nią — M.L.] nigdy nie zostało dokonane […], z punktu widzenia prawa międzynarodowego atak na nielegalne instalacje wojskowe przeciwnika był usprawiedliwiony […]. Zarówno cyber [ataki — M.L.], jak i konwencjonalne działania wojskowe zostały podjęte dopiero po uzasadnionych wysiłkach dyplomatycznych […]. Cyberuderzenia wyprzedzające zostały wymierzone w cele militarne: radar oraz systemy obrony przeciwlotniczej produkcji rosyjskiej […], co pozwoliło izraelskim myśliwcom wniknąć głęboko w syryjską przestrzeń powietrzną […]. W odróżnieniu od ataków konwencjonalnych, które nastąpiły później, cyberatak osiągnął swój wojskowy cel, sprawiając, iż siły obronne stały się bezradne, unikając [zarazem — M.L.] rozległych zniszczeń mienia lub utraty życia po obu stronach.

Z kolei Richard A. Clarke oraz Robert K. Knake (2010: 11) zauważyli:

> tak powinna być prowadzona wojna w erze informacyjnej, to była cyberwojna […], kiedy Izraelczycy zaatakowali Syrię, wykorzystali impulsy elektryczne i świetlne […] do przesyłu jedynek i zer, aby kontrolować to, co widziały radary syryjskiej obrony przeciwlotniczej. Zamiast wysadzać […], rezygnować z elementu zaskoczenia, w wieku cyberwojny Izraelczycy zagwarantowali [sobie — M.L.], że przeciwnik nie był nawet w stanie podjąć działań obronnych.

Choć słowa Clarke'a i Knake'a były sformułowane nieco na wyrost, to wydaje się, iż mieli słuszność co do tego, że był to wyraźny sygnał zmieniającego się oblicza operacji zbrojnych w dobie rewolucji informatycznej.

W wymiarze politycznym atak ten nie przyniósł pozornie poważniejszych konsekwencji. Ze strony izraelskiej przez dłuższy czas nie było w zasadzie żadnego oficjalnego potwierdzenia, że operacja *Orchard* w ogóle miała miejsce, media cytowały więc początkowo anonimowe wypowiedzi przedstawicieli władz w Tel Awiwie. Pierwszym politykiem, który przyznał, że rzeczywiście misja ta została zrealizowana, był dopiero lider opozycji Benjamin Netanyahu, który wspomniał o tym w swojej wypowiedzi z 19 września 2007 roku[141]. Nie potwierdziły tego jednak władze, które konsekwentnie odmawiały komentarza w tej sprawie[142]. Podobne stanowisko zajął reżim syryjski, który początkowo nie dość, że nie potwierdził tych wiadomości, to kategorycznie zaprzeczał istnieniu rodzimego programu atomowego. W ten sposób sprawę komentował m.in. ambasador w Stanach Zjednoczonych Imad Moustapha[143]. Sytuacja ta uległa częściowej zmianie dopiero pod koniec października, kiedy Ehud Olmert w jednej ze swoich wypowiedzi przeprosił Turcję na naruszenie jej przestrzeni powietrznej, choć i wówczas nie potwierdzono bezpośrednio, że atak rzeczywiście nastąpił[144]. Natomiast w grudniu do sprawy odniósł się Baszar al Assad, który stwierdził, że bombardowanie rzeczywiście miało miejsce, lecz zniszczone instalacje nie miały żadnego związku z programem atomowym[145].

Reasumując, warto zwrócić uwagę na trzy sprawy. Przede wszystkim, opierając się na powyższych doniesieniach, należy stwierdzić, iż operacja *Orchard* stanowiła udaną próbę zlikwidowania egzystencjonalnego zagrożenia Izraela. Odwołując się do teorii polityki zagranicznej, można zatem uznać, iż zrealizowano w ten sposób cel, jakim jest zapewnienie bezpieczeństwa państwa. Po drugie nie ma niestety do końca pewności, w jaki sposób misja ta została zrealizowana, dostępne informacje i wypowiedzi ekspertów pozwalają jednak sądzić, iż jednym z kluczowych czynników, które przyczyniły się do jej sukcesu, było odwołanie się do cyberataku (Rid, 2013: 42). Tym samym mogło to być kolejne po incydentach w Estonii potwierdzenie, że rola sieci komputerowych jako nowej domeny rywalizacji i konfrontacji państw zaczęła dynamicznie wzrastać. Wreszcie był to prawdopodobnie pierwszy przypadek w historii,

---

[141] H. Naylor: *Syria Tells Journalists Israeli Raid Did Not Occur*. „The New York Times" 11.10.2007: www.nytimes.com/2007/10/11/world/middleeast/11syria.html?rf=weorld; dostęp: 19.01.2014.

[142] S. Erlager: *Israel Silent on Reports of Bombing Within Syria*. „The New York Times" 15.10.2007: www.nytimes.com/2007/10/15/world/middleeast/15mideast.html; dostęp: 19.01.2014.

[143] T. Connolly: *Ambassador denies nuclear program in Syria*. The Dallas Morning News, 18.10.2007: www.dallasnews.com/sharedcontent/dws/news/world/stories/DN-syrian_18int.ART.State.Edition1.42ac4a2.html; dostęp: 19.01.2014.

[144] *Olmert Hints at Israel Air Raid on Syria*. The Associated Press, 28.10.2007: www.highbeam.com/doc/1Y1-111617633.html; dostęp: 19.01.2014.

[145] *Syrian Leader Reportedly Says His Country Was Approached by Head of Nuclear Black Market*. Fox News, 19.12.2007: www.foxnews.com/story/2007/12/19/syrian-leader-reportedly-says-his-country-was-approached-by-head-nuclear-black; dostęp: 19.01.2014.

kiedy działania w cyberprzestrzeni tak umiejętnie połączono z konwencjonalną operacją zbrojną, ponieważ włamanie do syryjskiego systemu obrony przeciwlotniczej miało konkretny militarny cel i pozwoliło na przeprowadzenie bez strat własnych udanego nalotu bombowego na obiekt w głębi wrogiego terytorium[146].

4.6. Cyberterroryzm w relacjach Izrael — USA — Iran *Stuxnet*, *Duqu* i *Flame*

Równolegle z omówionymi wyżej wydarzeniami w stosunkach izraelsko-syryjskich Tel Awiw stanął przed innym niezwykle poważnym zagrożeniem swojego bezpieczeństwa. Był nim program atomowy najbliższego sojusznika Damaszku — Iranu. Teheran miał dostęp do technologii jądrowych już od 1959 roku, kiedy to Stany Zjednoczone sprzedały mu pierwszy reaktor. Miał to być krok w kierunku budowy w tym kraju sieci 23 elektrowni atomowych do 1990 roku. Plan ten został oczywiście przekreślony przez rewolucję w 1979 roku, w której wyniku władzę objął ajatollah Chomeini (Squassoni, 2006: 1). Mimo to nowy reżim powoli kontynuował prace nad rozwojem technologii nuklearnych, co miało być, jak zauważyła Katarzyna Szymczyk (2012: 145) „elementem dynamicznego rozwoju państwa na drodze ku mocarstwowości w regionie, jak i czynnikiem kształtującym stosunki międzynarodowe państwa irańskiego z państwami regionu oraz z resztą świata". Tych aspiracji początkowo nie była jednak świadoma społeczność międzynarodowa. Jak stwierdził Marcin Andrzej Piotrowski (2012: 63—64), dopiero „z końcem lat dziewięćdziesiątych wywiady USA i Izraela weszły w posiadanie informacji o tajnych elementach wojskowego programu nuklearnego, w tym o pracach nad wzbogaceniem uranu, testach elementów niezbędnych do produkcji głowicy nuklearnej oraz studiach nad adaptacją do niej pocisku *Shahab 3*". Niemniej międzynarodowa opinia publiczna uzyskała wiedzę na ten temat dopiero w 2002 roku, kiedy irańska opozycja na konferencji prasowej przedstawiła dowody świadczące o zaawansowanych pracach reżimu w tej dziedzinie. Niedługo później, 13 grudnia 2002 roku, podobne oskarżenia wobec Teheranu wysunął Richard Boucher z Departamentu

[146] Warto dodać, że cyberataki w kolejnych latach na trwałe wpisały się w stosunki izraelsko-syryjskie. Gdy w 2011 roku w Syrii wybuchła wojna domowa, w którą od czasu do czasu angażowały się IDF, zaczęło dochodzić do regularnych incydentów teleinformatycznych. Za większością z nich stała grupa haktywistów patriotycznych z Syrian Electronic Army, broniąca reżimu Baszara al Assada. W maju 2013 roku podjęli oni np. nieudaną próbę zaatakowania systemów kontrolujących ujęcia wody w północnym Izraelu. Zob. J. Leyden: *Syrian Electronic Army' fails to crack Israeli water system*. „The Register" 31.05.2013: www.theregister.co.uk/2013/05/31/syrian_water_plant_hack_foiled; dostęp: 11.04.2014.

Stanu USA. Tego typu sytuacja w optyce państw zachodnich i Izraela oznaczała powstanie jednego z najpoważniejszych wówczas wyzwań dla bezpieczeństwa międzynarodowego. Chodziło tu nie tylko o egzystencjalne zagrożenie dla państwa żydowskiego czy wojsk amerykańskich na Bliskim Wschodzie, ale także o możliwość proliferacji broni masowego rażenia w regionie, biorąc pod uwagę zarówno rywalizację sunnicko-szyicką, jak i powiązania Teheranu z organizacjami terrorystycznymi. W tej sytuacji podjęto wielowymiarowe działania na rzecz zatrzymania tego programu, które zakładały przede wszystkim osiągnięcie porozumienia dyplomatycznego opartego na zamiennym stosowaniu zachęt oraz sankcji i gróźb, choć należy dodać, iż ani Izrael, ani Stany Zjednoczone nie wykluczały możliwości użycia sił zbrojnych. Czynione zabiegi nie osiągnęły jednak oczekiwanych rezultatów, co doprowadziło do zawiązania współpracy przez wszystkie kraje Rady Bezpieczeństwa ONZ oraz Niemcy (grupa E3/EU+3). Niestety kolejne porozumienia zawierane z Teheranem stosunkowo szybko okazywały się nieskuteczne. Podobnie było również z sankcjami nakładanymi przez Organizację Narodów Zjednoczonych, które nie skłoniły Teheranu do długotrwałych ustępstw (Lakomy, 2011b: 277—285).

Ta sytuacja oznaczała naturalnie poważne zagrożenie dla bezpieczeństwa narodowego Izraela. Przedłużanie się rokowań na linii E3/EU+3 — Teheran pozwalało Iranowi na stosunkowo dogodnych warunkach kontynuować prace nad technologiami, które, jak coraz częściej wskazywali badacze oraz służby wywiadowcze, mogły zostać wykorzystane do produkcji broni atomowej (zob. Kerr, 2013). Warto ponownie przywołać słowa Katarzyny Szymczyk (2012: 152), która pisała, iż Iran zachowywał się jak

> krnąbrne dziecko, kiedy to w 2006 roku nie przystał na korzystne dla siebie warunki, jak chociażby poparcie Wielkiej Brytanii, Rosji, Francji, Chin i USA w negocjacjach o przystąpienie do WTO, zniesienie sankcji gospodarczych, zakup nowych samolotów pasażerskich czy też dostęp do reaktorów o lekkiej wodzie na potrzeby energetyki cywilnej.

Z perspektywy Tel Awiwu była to sytuacja nie do przyjęcia, tym bardziej, że reżim ajatollahów to właśnie w nim upatrywał swojego *nemesis*. Co prawda w perspektywie historycznej Izrael i Iran w przeszłości blisko ze sobą współpracowały, jednak po 1979 roku uwarunkowania stosunków dwustronnych uległy diametralnej zmianie. Jak stwierdzili eksperci RAND National Defense Research Institute Dalia Dassa Kaye, Alireza Nader oraz Parisa Roshan (2011: IX), „irański reżim postrzega Izrael jako regionalnego rywala, nastawionego na podważenie jego systemu rewolucyjnego. Izrael postrzega Iran jako dominujące zagrożenie dla swojego bezpieczeństwa", z czego wynikają dodatkowe wyzwania zarówno w ujęciu strategicznym, jak i ideologicznym. Ich zdaniem uzyskanie przez Teheran broni atomowej w przyszłości oznaczałoby większe ryzyko wybu-

chu bezpośredniego konfliktu zbrojnego między nimi. W tym kontekście jednym z rozważanych przez Tel Awiw scenariuszy było wyprzedzające uderzenie, którego celem byłoby zniszczenie programu atomowego ajatollahów (Ibidem, s. IX). Możliwość urzeczywistnienia takiego scenariusza była tym bardziej prawdopodobna, iż reżim stosował niezwykle ostrą, antyizraelską retorykę. Szczególną rolę odegrał tu oczywiście Mahmoud Ahmedinejad, który wielokrotnie atakował Izrael, zapowiadając jego rychły upadek. W jednej ze swoich wypowiedzi stwierdził na przykład, że państwo to nie jest zakorzenione w regionie i powinno zostać „wyeliminowane"[147]. W innej zadeklarował z kolei, iż „każdy kto uzna Izrael, będzie się palił w ogniu furii narodu islamskiego"[148]. Tego typu semantyka była charakterystyczna dla polityków irańskich, którzy upatrywali w państwie żydowskim jednego ze swoich głównych wrogów. Tymczasem w Tel Awiwie przemówienia te były uznawane jedynie za potwierdzenie tego, iż Teheran rzeczywiście w XXI wieku stał się jednym z najpoważniejszych zagrożeń bezpieczeństwa Bliskiego Wschodu. Chodziło tu nie tylko o ewentualną możliwość wykorzystania broni atomowej, lecz również o powiązania reżimu szyickiego z Syrią i Hezbollahem, istniały bowiem obawy, iż tego typu środki mogłyby zostać użyte w sposób asymetryczny, przez wybrany podmiot pozapaństwowy. Przywódcy izraelscy obawiali się ponadto sytuacji, w której reagując na wzmocnienie pozycji Iranu, prace nad uzyskaniem ładunków jądrowych podjęłyby inne państwa regionu: Arabia Saudyjska, Turcja oraz Egipt[149].

W podobny sposób rozwój irańskiego programu atomowego postrzegał najbliższy sojusznik Izraela — Stany Zjednoczone. Jak stwierdziła Jadwiga Stachura (2007: 157), „ambicje Iranu, który dąży do uzyskania statusu mocarstwa nuklearnego, stanowiły zagrożenie dla przywódczej pozycji USA na Bliskim Wschodzie, bezpieczeństwa amerykańskich sojuszników (zwłaszcza Izraela), amerykańskich wpływów w regionie oraz stabilności i bezpieczeństwa dostaw surowców energetycznych". Podobne zdanie wyraził Radosław Bania (2012: 191), według którego Waszyngton postrzegał

> wejście przez Iran w posiadanie broni nuklearnej jako istotne zagrożenie dla własnych interesów w obszarze Zatoki, jak również bezpieczeństwa swoich sojuszników, w tym przede wszystkim Izraela. Kwestia ta jest również o tyle istotna, że Iran posiada rakiety balistyczne, które umożliwiają mu przeprowa-

[147] L. Charbonneau: *In New York, defiant Ahmedinejad says Israel will be 'eliminated'*. Reuters, 24.09.2012: www.reuters.com/article/2012/09/24/us-un-assembly-ahmadinejad-idUSBRE88N0HF20120924; dostęp: 20.01.2014.

[148] *5 Disturbing Quotes from Mahmoud Ahmedinejad*. The Centre for Israel & Jewish Affairs, 29.09.2010: www.cija.ca/middle-east/iran/5-disturbing-quotes-from-mahmoud-ahmadinejad-2; dostęp: 20.01.2014.

[149] Kahl, Dalton, Irvine, 2013; A. Ahmad: *The Saudi proliferation question*. „Bulletin of the Atomic Scientists" 17.12.2013: http://thebulletin.org/saudi-proliferation-question; dostęp: 20.01.2014.

dzenie ataku na każdy cel ulokowany w regionie Bliskiego Wschodu. Tym samym w obszarze bezpośredniego zagrożenia atakiem irańskim znajduje się nie tylko terytorium izraelskie, ale również siły zbrojne Stanów Zjednoczonych stacjonujące w obszarze Zatoki.

Waszyngton, podobnie jak Tel Awiw, był zatem żywotnie zainteresowany zatrzymaniem procesu wzbogacania uranu.

Mając na uwadze powyższe uwarunkowania, Izrael od początku rozważał możliwość zastosowania środków wojskowych. Gdy kolejne wysiłki dyplomatyczne nie przyniosły skutku, władze w Tel Awiwie coraz częściej zastanawiały się nad możliwością prewencyjnego uderzenia na Iran. Byłoby to więc powielenie scenariuszy znanych wcześniej z Iraku (operacja *Opera*) oraz omówionej już Syrii (operacja *Orchard*). Część komentatorów nalot na syryjski ośrodek atomowy uznała wręcz za element przygotowań do akcji przeciwko Teheranowi[150]. Dość dwuznaczną politykę prowadziła natomiast administracja amerykańska. George W. Bush co prawda nigdy nie wykluczył możliwości przeprowadzenia interwencji zbrojnej w tym kraju, w jednej ze swoich wypowiedzi z 2008 roku stwierdził bowiem, iż „wszystkie możliwości leżą na stole", niemniej nie była to opcja preferowana przez Biały Dom, który zdawał sobie sprawę, że tego typu operacja wiązałaby się z ogromnym ryzykiem, przede wszystkim dla wieloletnich amerykańskich wysiłków w Iraku oraz Afganistanie. Dlatego też Waszyngton starał się tonować izraelskie zamiary przeprowadzenia interwencji wojskowej o czym świadczyła chociażby odmowa przekazania mu bomb typu GBU-28 *Bunker Buster*, które byłyby zdolne do zniszczenia podziemnych irańskich instalacji (Lakomy, 2011b: 280).

Ostrożność w sprawie ewentualnej interwencji izraelskiej lub amerykańskiej wynikała jeszcze z kilku innych przesłanek. Przede wszystkim Teheran, czerpiąc z doświadczeń Iraku i Syrii, w odpowiedni sposób zaprojektował swój program atomowy, lokalizując kluczowe instalacje na całym terytorium kraju (zob. Kerr, 2009). W sumie składał się on z kilkunastu ośrodków, wśród których największe znaczenie miały stacja wzbogacania uranu w Qom, elektrownia atomowa w Bushehr, stacja przetwarzania uranu w Isfahan, centrum wzbogacania uranu w Natanz, fabryka ciężkiej wody w Arak oraz centra badań atomowych m.in. w Teheranie oraz Bonab (Szymczyk, 2012: 148). Po drugie posiadał bardzo duży potencjał wojskowy, który nawet dla IDF stanowił znaczne wyzwanie. Składało się na niego ponad pół miliona żołnierzy, ze stosunkowo silną obroną przeciwlotniczą, wyposażoną głównie w sprzęt produkcji rosyjskiej (zob. Burgess, 2010). Po trzecie istotnym czynnikiem utrudniającym ewentualną interwencję zbrojną była odległość. Z perspektywy Izraela problemem był nie tylko przelot nad z reguły wrogimi państwami arabskimi, lecz również ograniczony

[150] P. Beaumont: *Was Israeli raid a dry run for attack on Iran?* „The Guardian" 16.09.2007: www.theguardian.com/world/2007/sep/16/iran.israel; dostęp: 20.01.2014.

zasięg samolotów F-15 i F-16. Było to tym bardziej widoczne, iż, jak wspomniano, należało jednocześnie zbombardować wiele odległych od siebie ośrodków (m.in. w Bushehr czy Natanz)[151]. Po czwarte znaczne wątpliwości wiązały się z wielowymiarowymi zdolnościami Iranu do odpowiedzi na interwencję zbrojną. Z jednej strony wskazywało się tutaj na szeroki asortyment rakiet balistycznych, z drugiej obawiano się również ewentualnego zablokowania przez reżim ajatollahów Cieśniny Ormuz, co mogłoby w efekcie doprowadzić do radykalnego podniesienia cen surowców energetycznych. Wśród innych wymieniano również możliwą reakcję Hezbollahu czy zamachy terrorystyczne[152]. Warto tutaj przytoczyć słowa Michaela Eisenstadta i Michaela Knightsa, którzy przewidywali jeszcze inne scenariusze: ostrzał rakietami balistycznymi izraelskiego reaktora atomowego w Dimonie, ataki na sąsiednie kraje, które popierały działania Tel Awiwu, ataki na bazy Stanów Zjednoczonych w regionie czy też porwania amerykańskich obywateli (Eisenstadt, Knights, 2012: 2). W ciekawy sposób do tych zagadnień odnieśli się również eksperci z amerykańskiego Congressional Research Service Jim Zanotti, K. Katzman, J. Gertler i Steven A. Hildreth (2012: 41—43), którzy doszli do wniosku, że istniały uzasadnione wątpliwości co do tego, czy wybór opcji militarnej mógłby w ogóle zakończyć się zatrzymaniem irańskiego programu atomowego. Wiele czynników wskazywało na fakt, że udane bombardowania opóźniłyby program jedynie od 3 do 5 lat.

W tym kontekście powielenie działań przećwiczonych przez Izrael w Iraku i Syrii w przypadku Iranu wiązało się więc z szeregiem fundamentalnych problemów. Wysokie ryzyko poniesienia porażki, a także ewentualne koszty tej operacji skłoniły Izrael i sprzymierzone z nim Stany Zjednoczone do poszukiwania alternatyw, które mogłyby doprowadzić do zatrzymania lub chociaż spowolnienia procesu wzbogacania uranu przez Iran. Było to tym istotniejsze, iż na przełomie pierwszej i drugiej dekady XXI wieku USA pozostawały raczej sceptyczne wobec unilateralnej akcji zbrojnej ze strony Tel Awiwu, obawiając się potencjalnych negatywnych konsekwencji dla swoich interesów w regionie (Kaye, Nader, Roshan, 2011: 43—46). W tej sytuacji jednym z instrumentów, które zaczęto intensywnie stosować, była wzmożona aktywność wywiadowcza, której efektem były zabójstwa wysokich rangą naukowców odgrywających kluczowe role w programie nuklearnym ajatollahów. W latach 2007—2012 w ten sposób zginęło w sumie pięciu specjalistów z zakresu atomistyki[153]. Utrudniło to oczywiście warunki prowadzenia badań, lecz ich bynajmniej nie zatrzymało.

---

[151] *'Azerbaijan allows Israel to use its air bases near Iran border'*. „Israel Hayom", 29.03.2012: www.israelhayom.com/site/newsletter_article.php?id=3718; dostęp: 20.01.2014.

[152] *Weighing Benefits and Costs of Military Action Against Iran*. Iran Project. New York 2012, s. 33—36; R. Hirschfeld: *Iran Warns of Strait of Hormuz Closure if US Chooses 'War'*. Israel National News, 25.01.2013: www.israelnationalnews.com/News/News.aspx/164555; dostęp: 20.01.2014.

[153] *Mossad hit-squads behind Iran scientists' murders — US official*. RT.com, 09.02.2012: http://rt.com/news/iranian-scientists-assassinations-israel-923; dostęp: 20.01.2014.

Jak wspomniano wcześniej, na przełomie pierwszej i drugiej dekady XXI wieku Izrael posiadał już pewne doświadczenie oraz rosnący potencjał naukowo-techniczny w zakresie wykorzystania cyberprzestrzeni do działań na arenie międzynarodowej[154]. Z jednej strony udowodniła to poniekąd omówiona już operacja *Orchard*, z drugiej natomiast świadczyły o tym statystyki. W 2011 roku w rankingu Międzynarodowego Związku Telekomunikacyjnego *ICT Development Index* Tel Awiw zajmował wysokie, 27. miejsce, wyprzedzając m.in. Włochy oraz Hiszpanię (*Measuring the Information Society*, 2012: 7). Nie oddawało to jednak jego rzeczywistych zdolności, które rozwijał przede wszystkim pod względem wywiadowczych i wojskowych zastosowań technologii teleinformatycznych. Można tutaj przywołać artykuł z czasopisma „Defense Technology International" z początku 2010 roku, w którym zauważono, iż kraj ten, obok Stanów Zjednoczonych i Francji, był liderem, jeśli chodzi o możliwości prowadzenia cyberwojny. Świadczyły o tym m.in. osiągnięcia takich przedsiębiorstw, jak Converse and Nice Systems, będącego liderem na światowym rynku sieci podsłuchowych, czy Checkpoint Software, mającego znaczny dorobek w zakresie zabezpieczania sieci komputerowych. Podkreślono przy tym, iż w ramach izraelskich służb wywiadowczych działały wyspecjalizowane zespoły odpowiedzialne za prowadzenie walki w cyberprzestrzeni. O szczególnym znaczeniu ICT w izraelskiej polityce bezpieczeństwa świadczyły również wypowiedzi szefa wywiadu wojskowego, gen. Amosa Yadlina, który stwierdził, iż „wykorzystanie sieci komputerowych do działań szpiegowskich jest tak ważne dla dzisiejszej wojny, jak pojawienie się wsparcia lotniczego dla wojny na początku XX wieku". Podkreślił przy tym, że „sfera cyberwojny w pełni pasuje do izraelskiej doktryny obronnej"[155]. W tym kontekście Alon Ben-David zauważył, iż tak duży nacisk położony przez Tel Awiw na rozwój zdolności w tej dziedzinie wynikał w głównej mierze z coraz większego przygotowania organizacji terrorystycznych, takich jak Hamas czy Hezbollah, do działań w Internecie[156].

W połowie czerwca 2010 roku na specjalistycznych portalach zajmujących się bezpieczeństwem sieci komputerowych zaczęły się pojawiać pierwsze informacje o odkryciu nowego typu złośliwego oprogramowania. Jako pierwsze natrafiło na niego 17 czerwca białoruskie przedsiębiorstwo VirusBlokAda, które specjalizowało się w oprogramowaniu antywirusowym. Analitycy VBA Oleg Kuprejew oraz Sergiej Ulasen przygotowali wstępny, 7-stronicowy raport zawierający jego podstawową charakterystykę. Stwierdzono tam, iż powinien on zostać zaliczony do kategorii najgroźniejszych programów z dwóch powodów. Po pierwsze zaraz po zainfekowaniu komputera zaczynał się ukrywać,

[154] Szerzej na ten temat: Baram, 2013, s. 23—43.

[155] *Israel Adds Cyber-Attack to IDF*. DefenseTech, 11.02.2010: http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf; dostęp: 20.01.2014.

[156] *Israelis Very Serious About Cyberwar*. DefenseTech, 02.04.2010: http://defensetech.org/2010/04/02/israelis-very-serious-about-cyberwar; dostęp: 20.01.2014.

wykorzystując do tego nadal nienaprawione błędy systemu operacyjnego. Po drugie stosował techniki, które wprowadzały w błąd dotychczasowe metody działania programów typu *antirootkit*[157]. Początkowo reakcja innych ekspertów i korporacji zajmujących się walką ze złośliwym oprogramowaniem była niewielka. Dopiero po kilku tygodniach zaczęto podejmować działania na rzecz naprawy błędów w oprogramowaniu, które wykorzystywał program określany wówczas jako *W32.Temphid*. Jako pierwsza nowych odkryć dokonała 17 lipca firma ESET. W dwa dni później znana korporacja Symantec zmodyfikowała nazwę nowego programu na *W32.Stuxnet*. Wtedy też zareagował Siemens, który dostrzegł w końcu coraz częściej pojawiające się doniesienia, iż nowy robak infekował przede wszystkim produkowane przez niego systemy przemysłowe SCADA (Supervisory Control and Data Acquisition) typu WinCC. 20 lipca Symantec oświadczyło, iż odkryło, że *Stuxnet* porozumiewa się ze zdalnymi serwerami dowodzenia i kontroli (C&C). Na początku sierpnia zareagowała również korporacja Microsoft, która w opublikowanym biuletynie MS10-046, zaproponowała kilka „łat" błędów w swoim oprogramowaniu, które dotychczas wykorzystywał *Stuxnet*.

Nowy robak stał się obiektem pogłębionych badań, które rodziły jednak zasadnicze trudności, stosunkowo szybko okazało się bowiem, iż jest on niezwykle skomplikowany, zrozumienie wszystkich jego funkcji, nawet przez biegłych informatyków, musiało zatem zająć wiele czasu. W związku z tym pierwszy raport wyjaśniający podstawowe sposoby działania oraz cechy *Stuxnetu* opublikowano dopiero 30 września 2010 roku. Pominięto w nim jednak, jak się szybko okazało, kilka istotnych zagadnień związanych z wykorzystaniem jeszcze „niezałatanych" (*patch*) błędów w kodzie systemów Microsoftu (*Stuxnet Part I*, 2011: 5—7). To właśnie wtedy sprawą na dobre zainteresowały się światowe media, które zaczęły się zastanawiać nad pochodzeniem oraz znaczeniem nowego typu złośliwego oprogramowania, wzbudzającego tak duże kontrowersje w środowisku naukowym. Unikalną cechą prowadzonej wówczas debaty była świadomość, iż pełne przeanalizowanie programu okazało się niespotykanym dotychczas wyzwaniem. Jak zastrzegli analitycy Symantec we wstępie do swojego raportu z lutego 2011 roku, „choć większość analizy jest gotowa, *Stuxnet* jest niewiarygodnie wielkim i kompleksowym zagrożeniem". Nicolas Falliere, Liam O Murchu oraz Eric Chien stwierdzili, iż sława tego robaka była uzasadniona. Ich zdaniem był on jednym z najbardziej złożonych zagrożeń komputerowych, jakie kiedykolwiek analizowali (Falliere, O Murchu, Chien, 2011: 1). Podobnego zdania byli inni specjaliści. Alan Bentley z Lumension zauważył na przykład, iż jest to „najbardziej wyrafinowany" złośliwy program, jaki kiedykol-

[157] O. Kuprejev, U. Sergey: *Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review*. VirusBlokAda 2010., s. 7: www.wilderssecurity.com/attachment.php?attachmentid=219888&d=1279012965; dostęp: 20.01.2014.

wiek odkryto[158]. Zrozumienie zasad jego działania wymagało więc czasu oraz, co niezwykłe, wiedzy wykraczającej poza obszar informatyki, zaprojektowano go bowiem, jak wspomniano, z myślą o zainfekowaniu komputerowych systemów kontroli przemysłowej produkcji Siemensa — WinCC, działających w środowisku Windows (XP, Vista, 7 itp.). W założeniu miał on zmieniać sposoby działania programowalnych sterowników logicznych (PLC — Programmable Logic Controllers), będących komputerami wykorzystywanymi w procesach przemysłowych. Ich znaczenie trafnie ujął Marcin Pawlak, według którego „sterowniki programowalne stanowią dzisiaj podstawowy element sterujący zautomatyzowanych procesów technologicznych, obecnych niemalże w każdej gałęzi przemysłu"[159]. Potencjalnie oznaczało to, iż kod robaka mógł zaszkodzić elementom infrastruktury krytycznej, której funkcjonowanie jest częstokroć oparte właśnie o PLC. *Stuxnet*, jak się okazało po pewnym czasie, miał jednak bardziej sprecyzowany cel, którym były wirówki do wzbogacania uranu typu IR-1 wykorzystywane w irańskim programie atomowym[160]. Kolejne prace badawcze podjęte przez szereg ośrodków badawczych oraz korporacje sektora ICT wykazały, iż większość infekcji wystąpiła w Iranie. Z ok. 100 000 zarażonych komputerów na całym świecie aż 60 000 znajdowało się właśnie tam. Ponadto te, które posiadały zainstalowane oprogramowanie Siemensa, również w większości (67,6%) były zlokalizowane w państwie ajatollahów (Falliere, O Murchu, Chien, 2011: 6).

W związku z tymi doniesieniami zaczęto się zastanawiać nad pochodzeniem oraz docelowymi funkcjami, które miał pełnić *Stuxnet*. Gdy zrozumiano podstawowe właściwości techniczne nowego programu, część badaczy uznała, iż jego twórcy za główny cel obrali irańską elektrownię atomową w Bushehr, budowaną m.in. przy współpracy z Rosjanami[161]. Inne doniesienia wskazywały natomiast, że cyberatak skupił się na instalacjach w Natanz[162]. Spekulacje światowych mediów dodatkowo pogłębiła reakcja samego Teheranu. Prezydent Mahmoud Ahmedinejad potwierdził w listopadzie 2010 roku, iż *Stuxnet*, jakkolwiek został zatrzymany, wyrządził pewne szkody programowi atomowemu. Była to

[158] J. Halliday: *Stuxnet worm is the 'work of a national government agency'*. „The Guardian" 24.09.2010: www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency; dostęp: 24.01.2014.

[159] M. Pawlak: *Sterowniki programowalne*. Politechnika Wrocławska, s. 2: www.dbc.wroc.pl/Content/7791/Pawlak_Sterowniki_programowalne.pdf; dostęp: 24.01.2014.

[160] Szerzej o wirówkach: J. Kubowski: *Wirówka do wzbogacania uranu*. Nuclear.pl: www.nuclear.pl/publikacje/pliki/Wirowka.pdf; dostęp: 24.01.2014.

[161] C. Caughlin: *Stuxnet virus attack: Russia warns of 'Iranian Chernobyl'*. „The Telegraph" 16.01.2011: www.telegraph.co.uk/news/worldnews/europe/russia/8262853/Stuxnet-virus-attack-Russia-warns-of-Iranian-Chernobyl.html; dostęp: 24.01.2014.

[162] Y. Katz: *Stuxnet may have destroyed 1,000 centrifuges at Natanz*. „The Jerusalem Post" 24.11.2010: www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz; dostęp: 24.01.2014.

odpowiedź na wiadomości o czasowym wstrzymaniu przez Iran procesu wzbogacania uranu[163]. Równolegle w mediach i środowisku naukowym coraz częściej zaczęły pojawiać się spekulacje na temat tego, kto stał za tymi incydentami. Ekspert korporacji Kaspersky Lab David Emm stwierdził, że poziom skomplikowania *Stuxnetu*, jego cel oraz wymagane do jego stworzenia dane wywiadowcze sugerowały wyraźny udział aktora państwowego[164]. Wśród potencjalnych jego twórców w mediach wymieniano przede wszystkim Stany Zjednoczone i/lub Izrael[165]. Wszystkie te informacje ujawnione w drugiej połowie 2010 roku wskazywały więc jednoznacznie, iż *casus* wirusa *Stuxnet* był w swojej istocie wyjątkowy. W konsekwencji zaczęły się pojawiać pierwsze głosy mówiące o np. o wejściu w „trzecią erę" cyberprzestępczości, charakteryzującą się wykorzystaniem Internetu w celach politycznych, ekonomicznych lub wojskowych. W ten sposób incydenty te wyjaśniał przedstawiciel korporacji Sophos Graham Cluley[166].

W prowadzonej wówczas międzynarodowej debacie na ten temat pojawiło się jednak sporo przekłamań i uproszczeń, które nie pozwalały na wyciągnięcie precyzyjnych wniosków. W związku z tym, warto odwołać się do pogłębionych analiz, które opracowano w ciągu kolejnych trzech lat po odkryciu *Stuxnetu*. Wyjaśniły one nie tylko techniczne właściwości samego robaka, rzeczywiste skutki jego działania, lecz również odpowiedziały na pytanie, kim byli jego twórcy.

Przede wszystkim należałoby szerzej omówić proces jego utworzenia i ewolucji. Jak zauważył niemiecki analityk Ralph Langner (2013: 5), *de facto* opracowano dwie jakościowo nieco odmienne wersje robaka *Stuxnet*. Źródła pierwszej, pierwotnej sięgają roku 2007, kiedy niezidentyfikowany użytkownik zamieścił na platformie Virustotal elementy jego kodu. Jak się później okazało, był to właśnie program, który zaatakował irańskie elektrownie atomowe. Co ciekawe, wówczas żaden z ekspertów nie zwrócił na niego większej uwagi, co wiązało się z faktem, iż jego specyfika techniczna odróżniała go od głównego nurtu złośliwego oprogramowania. Z jednej strony stosował on bardzo prosty sposób infekowania komputerów, głównie przy użyciu pamięci przenośnych USB, z drugiej jednak do jego unikalnych cech należała zdolność ukrycia się przed oprogramowaniem antywirusowym oraz możliwość wpływania na funkcjonowanie wirówek wzbogacających uran. *Stuxnet* w pierwotnej wersji miał za zadanie wytwarzać w nich podciśnienie, które w założeniu miało prowadzić do pozornie naturalnych awarii infrastruktury przemysłowej. Ponadto sposób jego

[163] *Ahmedinejad admits centrifuges damaged by virus*. „The Jerusalem Post" 29.11.2010: www.jpost.com/Iranian-Threat/News/Iran-nuke-enrichment-stopped-Stuxnet-worm-suspected; dostęp: 24.01.2014.

[164] J. Halliday: *Stuxnet worm is the 'work of a national government agency'*, op.cit.

[165] T. Worstall: *Stuxnet Was a Joint US/Israeli Project*. „Forbes" 01.06.2012: www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project; dostęp: 24.01.2014.

[166] J. Halliday: *Stuxnet worm is the 'work of a national government agency'*…, op.cit.

działania w systemach teleinformatycznych był na tyle specyficzny, iż można go było łatwo pomylić z legalnie zainstalowanym oprogramowaniem. Zdaniem Ralpha Langnera świadczyło to o tym, że jego twórcy chcieli działać w ukryciu oraz uniknąć scenariusza, w którym wszystkie irańskie wirówki zostałyby zniszczone naraz. Taki plan wynikał z kolei ze świadomości, iż Teheran posiadał ich znaczne zapasy, a więc dekonspiracja robaka jedynie na krótko zatrzymałaby proces wzbogacania uranu, tymczasem symulowanie „naturalnych" awarii mogło mieć bardziej długofalowe i korzystniejsze skutki (Ibidem, s. 5—11). Niemniej w 2009 roku, kiedy *Stuxnet* już działał w Iranie, jego twórcy doszli do wniosku, iż należałoby stworzyć jego nową wersję. Mogło to wynikać zarówno z mniejszych niż zakładano efektów, jak i problemów z właściwym zainfekowaniem wszystkich wrażliwych systemów. Możliwe też, że po prostu chciano spróbować nowych sposobów działania w cyberprzestrzeni. Nowy, zaktualizowany program odkryto dopiero w 2010 roku. Jak się szybko okazało, zdecydowanie bardziej przypominał on popularne złośliwe oprogramowanie, był więc o wiele łatwiejszy do wykrycia (Ibidem, s. 10—11).

Nowa wersja, na którą natrafiła wspomniana VirusBlokAda, została wyposażona w szereg nieodkrytych jeszcze *exploitów* „dnia zerowego", a także skradzionych certyfikatów bezpieczeństwa. Dzięki temu *Stuxnet* był postrzegany przez systemy korporacji Microsoft jako sterownik niezbędny do funkcjonowania wybranych urządzeń komputerowych. W swojej dojrzałej wersji posiadał kilka cech, które świadczyły o jego wyjątkowości, złożoności, a co za tym idzie o możliwościach sparaliżowania irańskiej infrastruktury przemysłowej. Można tu wymienić za Erikiem Byresem, Andrew Ginterem oraz Joelem Langillem (2011: 6—7) następujące kwestie:

1. Głównym nośnikiem robaka były różne typy pamięci przenośnych.
2. Rozpowszechniał się w danym ośrodku za pomocą różnych kanałów sieciowych.
3. Wyszukiwał funkcjonujące w systemach programy antywirusowe i modyfikował ich działanie w taki sposób, aby uniknąć wykrycia.
4. Kontaktował się z serwerami dowodzenia i kontroli (C&C) za pomocą Internetu w celu pobrania aktualizacji oraz dodatkowych instrukcji.
5. Modyfikował programowalne sterowniki logiczne, co prowadziło do usterek fizycznych urządzeń przemysłowych (wirówek IR-1).
6. Ukrywał modyfikacje dokonane w programowalnych sterownikach logicznych przed administratorami systemów.
7. Wykorzystywał certyfikaty skradzione jednemu z dwóch głównych producentów sprzętu komputerowego, przez co instalacja robaka nie prowadziła do pojawienia się ostrzeżeń w systemie.
8. Jeśli konkretny komputer nie posiadał oprogramowania produkcji Siemensa, po dokonaniu replikacji na inne nośniki i komputery robak sam usuwał się z twardego dysku (Byres, Ginter, Langill, 2011, s. 6—7).

Jego funkcjonowanie zdaniem badaczy University of Twente generalnie składało się z trzech faz. Pierwszą była proliferacja, co odbywało się za pomocą pamięci przenośnych (USB), innych nośników pamięci, przez dostępne sieci, a także udostępniane foldery. Tak skomplikowany sposób rozpowszechniania wynikał z tego, że głównym celem *Stuxnetu* był sabotaż systemów SCADA, które z reguły odcięte są od Internetu. Druga faza obejmowała uzyskanie dostępu do programowalnych sterowników logicznych (PLC). Trzecią fazą był natomiast sabotaż infrastruktury przemysłowej[167]. Ten ostatni etap był oczywiście kluczowy dla zrealizowania fundamentalnego celu, który przyświecał twórcom *Stuxnetu*. Był nim wspomniany już sabotaż wirówek do wzbogacania uranu typu IR-1. Odbywało się to na dwa sposoby. Zgodnie z pierwszym, bardziej zaawansowanym, lecz prawdopodobnie nieco mniej skutecznym, program modyfikował funkcjonowanie zaworów połączonych z wirówkami w taki sposób, aby przepływający gaz nie miał jak się ulotnić. W konsekwencji prowadziło to do wzrostu ciśnienia, a tym samym do powstawania częstych usterek w IR-1. Równolegle *Stuxnet* manipulował działalnością czujników analogowych, które miały monitorować ciśnienie w wirówkach. Tym samym administratorzy oraz inżynierowie otrzymywali błędne dane wyjściowe, co nie pozwalało im odkryć rzeczywistych powodów awarii. Warto dodać, że tego typu ataki były z założenia ograniczone czasowo, ich przedłużenie mogło się bowiem zakończyć eksplozją (Langner, 2013: 9—10). Drugi sposób, który zastosowano zdecydowanie później (w 2009 roku), był nieco mniej zaawansowany, lecz prawdopodobnie bardziej skuteczny. Ten wektor ataku polegał przede wszystkim na zainfekowaniu innego komponentu systemu przemysłowego — układu napędowego wirówek (Centrifuge Drive System — CDS), kontrolującego szybkość obrotu wirników. Średnia dla wirówek IR-1 wynosiła ok. 63 000 obrotów na minutę, tymczasem *Stuxnet* regularnie zwiększał ich prędkość o ok. 1/3 do poziomu 84 600 obrotów na minutę, co w konsekwencji prowadziło do powstawania częstych uszkodzeń (Ibidem, s. 11—13). Ze względu na brak miarodajnych odczytów czujników nadzorcy uznawali awarie za konsekwencję zastosowania niskiej jakości materiałów.

Ten unikalny i niezwykle skomplikowany sposób działania robaka pozwolił środowisku naukowemu na sformułowanie szeregu interesujących wniosków na temat incydentów teleinformatycznych w Iranie. Potwierdzono, że *Stuxnet* był wymierzony w program atomowy Teheranu, wszystkie swoje funkcje związane z sabotażem wykonywał bowiem jedynie w środowisku specyficznym dla ośrodków działających w państwie ajatollahów. Gdy nie natrafił na odpowiednie warunki, nie czynił żadnych szkód.

---

[167] A. Kolesnichenko, P.-T. de Boer, A. Remke, E. Zambon, B.R. Haverkort: *Is Quantitative Analysis of Stuxnet Possible?* „QEST 2011": http://eprints.eemcs.utwente.nl/20911; dostęp: 27.01.2014.

Przytoczone powyżej informacje pozwalają stwierdzić, iż po raz pierwszy w historii zastosowanie złośliwego oprogramowania doprowadziło do powstania rzeczywistych strat materialnych w infrastrukturze krytycznej państwa. W tym wypadku były to posiadające strategiczne znaczenie instalacje nuklearne Teheranu (Even, Siman-Tov, 2012: 38). Pisał o tym m.in. Radosław Bania (2012: 197), który zauważył, że została tu przekroczona pewna granica. Jego zdaniem „wykazano, że jest możliwe zadanie strat materialnych poprzez atak na zasoby komputerowe państwa". Z kolei analitycy z brytyjskiego Chatham House stwierdzili: „identyfikacja wirusa *Stuxnet* może stanowić otwarcie nowego etapu wykorzystania cyberprzestrzeni do strategicznego efektu [jakim jest — M.L.] neutralizacja międzynarodowego zagrożenia" (Cornish, Livingstone, Clemente, Yorke, 2010: 7). Słuszność tych opinii potwierdziła zresztą reakcja reżimu ajatollahów. Jak już wspomniano, jako pierwszy na ten temat wypowiedział się w sposób dość ogólnikowy prezydent Mahmoud Ahmedinejad. Przyznał wówczas, że złośliwy program komputerowy uszkodził niektóre wirówki do wzbogacania uranu[168]. W kwietniu 2011 roku incydent ten potwierdził również Gholam Reza Jalali, odpowiedzialny w Iranie za zwalczanie sabotażu. Winą za stworzenie złośliwego robaka obarczył on wówczas Izrael oraz Stany Zjednoczone[169]. Precyzyjniejsze i potwierdzające te słowa dane zebrał Institute for Science and International Security. Według raportu tego ośrodka badawczego w wyniku działania robaka na przełomie 2009 i 2010 roku zniszczeniu uległo ok. 1000 wirówek w Natanz z ogólnej liczby 9000 funkcjonujących tam maszyn. Na tej podstawie ISIS stwierdziło, że dzięki niemu na wiele miesięcy część irańskiej infrastruktury wzbogacającej uran pozostała bezczynna. Sytuacja ta mogła doprowadzić do większych trudności Teheranu w zdobyciu niezbędnych surowców do budowy nowych wirówek, niemniej zdaniem ekspertów *de facto* stosunkowo szybko wymieniono uszkodzone elementy na nowe. Co więcej, niektóre sektory instalacji w Natanz nie były w ogóle sabotowane (Albright, Brannan, Walrond, 2011; 3—4). W tym kontekście warto również przywołać słowa Freda Schreiera, który zwrócił uwagę na fakt, że po ujawnieniu *Stuxnetu* nie dokonano w terminie otwarcia elektrowni atomowej w Bushehr, co pierwotnie planowano na drugą połowę sierpnia 2010 roku[170]. Bez względu na te niuanse wśród badaczy panuje generalnie zgoda co do tego, że twórcom robaka udało się spowolnić program nuklearny Iranu.

---

[168] M. Clayton: *Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program*. „The Christian Science Monitor" 30.11.2010: www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program; dostęp: 27.01.2014.

[169] *Iran admits Stuxnet's damage*. Homeland Security News Wire, 18.04.2011: www.homelandsecuritynewswire.com/iran-admits-stuxnets-damage; dostęp: 27.01.2014.

[170] Co ciekawe, Fred Schreier (2015: 88) podał zdecydowanie większą liczbę zniszczonych wirówek irańskich: między 5084 a 8856. Ponadto zauważył, że nie wiadomo, czy podobnych problemów napotkał ośrodek wzbogacania uranu w Fordow, gdzie skutki działania robaka komputerowego mogły być podobne.

Na tej podstawie powstaje więc pytanie, kto w rzeczywistości opracował ten nowy rodzaj złośliwego oprogramowania. Wykluczono udział podmiotów pozapaństwowych, które nie mogły posiadać wystarczającego potencjału finansowego, technicznego oraz *know-how*, aby stworzyć tak wysoce wyspecjalizowany program (zob. Foltz, 2012: 45—46). Wynikało to z faktu, iż oprócz wybitnej wiedzy z zakresu informatyki twórcy *Stuxnetu* posiadali również specjalizacje z innych dziedzin i dyscyplin, w tym m.in. atomistyki oraz inżynierii przemysłowej, mieli ponadto dostęp do szczegółowych informacji wywiadowczych. W ciekawy sposób kwestie te przedstawił przywoływany już Ralph Langner. Jego zdaniem kod robaka był po pierwsze na tyle skomplikowany i wyspecjalizowany, że bez gruntownego jego przetestowania na istniejących już instalacjach nie było żadnej gwarancji jego skuteczności. Po drugie takie testy mogły być przeprowadzone tylko w sytuacji, w której twórcy mieli dostęp do w pełni funkcjonalnej kaskady wirówek IR-1 oraz uranu. Po trzecie sprawcy mieli ogromną wiedzę nie tylko na temat zasad funkcjonowania tego typu infrastruktury wzbogacającej uran, lecz również sposobów jej działania w Iranie. Na tej podstawie Langner (2013: 10, 20) ukuł następujące twierdzenie: „Ktokolwiek przekazał wymagane informacje, mógł równie dobrze wiedzieć, jakie są ulubione dodatki do pizzy miejscowego szefa inżynierów".

Po wykluczeniu udziału podmiotów pozapaństwowych powstało więc pytanie, który z rządów mógł dokonać tego cyberataku. Trafnie zagadnienia te ujął Radosław Bania (2012: 196), według którego

> należałoby zadać pytanie, kto w największym stopniu odniósłby korzyści z ataku na irański program atomowy. Pamiętajmy jednak, że sytuacja, w której „każdy atak cybernetyczny jest anonimowy", powoduje, że w tym względzie jesteśmy skazani na spekulacje, opierając argumentację nie na mocnych dowodach, ale jedynie na poszlakach. Przy tak postawionym pytaniu najpoważniejsze podejrzenia kierują się ku Stanom Zjednoczonym i Izraelowi.

Generalnie od samego początku zdecydowana większość ekspertów i komentatorów wskazywała właśnie na te dwa państwa, które posiadały zarówno motyw, jak i wystarczający potencjał. Jednocześnie jednak pojawiały się i inne, mniej zasadne sugestie, dotyczące m.in. odpowiedzialności Chińskiej Republiki Ludowej[171]. Na tym tle warto więc przytoczyć najważniejsze argumenty, które świadczyły o zaangażowaniu Waszyngtonu i Tel Awiwu w projekt *Stuxnet*. Jak wspomniano wyżej, oba kraje miały wyraźny motyw, wynikający z obaw przed powstaniem irańskiej broni jądrowej. Ponadto zarówno USA, jak i Izrael należały do światowej czołówki państw posiadających zdolności do prowadzenia walki z cyberprzestrzeni, posiadały też odpowiednią infrastrukturę do tego, aby

[171] J. Carr: *Stuxnet's Finnish-Chinese Connection*. „Forbes" 14.12.2010: www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection; dostęp: 27.01.2014.

program odpowiednio opracować, a następnie przetestować jego skuteczność. Warto tutaj odwołać się do informacji podanych przez „The New York Times", według których odbywało się to w izraelskiej elektrowni atomowej w Dimonie. Zdaniem gazety oba państwa miały ze sobą ściśle współpracować, przy czym w niektórych fazach projektu bezwiednie mieli uczestniczyć także eksperci niemieccy oraz francuscy[172]. Wiadomości te potwierdził również były pracownik amerykańskiego wywiadu Edward Snowden[173]. O udziale Izraela w pracach nad *Stuxnetem* świadczyły również pewne elementy kodu tego oprogramowania. Z jednej strony, jak odkryli specjaliści korporacji Symantec, występowała w nim interesująca liczba 19790509, która determinowała infekcje danego komputera. Początkowo nie zwracano na to większej uwagi, uznając to za losowy ciąg cyfr. Później jednak zauważono, iż koresponduje to z ważną datą w historii stosunków izraelsko-irańskich — zamordowaniem przez rewolucjonistów islamskich pierwszego irańskiego Żyda Habiba Elghaniana, będącym pierwszym z całej serii wydarzeń, które doprowadziły do ucieczki z tego kraju ponad 100 000 osób tej narodowości (Falliere, O Murchu, Chien, 2011: 18). Z drugiej strony odnaleziono tam również interesujący zwrot *myrtus* oznaczający po łacinie mirt zwyczajny. Jak zauważyli analitycy, mogło być to odniesienie do historii Estery ze Starego Testamentu dotyczącej perskiego spisku wymierzonego w Żydów. Wskazywał na to fakt, iż jej prawdziwe imię brzmiało Hadassah, co w języku hebrajskim jest tożsame właśnie ze słowem *mirt*[174]. Warto jednak zaznaczyć, iż słowo *myrtus* mogło *de facto* oznaczać coś zupełnie innego — zwrot *MyRTUs*, czyli folder zatytułowany „Moje RTU" (Remote Terminal Units) (*Stuxnet Part I*, 2011: 27). Niemniej biorąc pod uwagę wszystkie przytoczone wyżej fakty oraz wskazówki, nie powinno być wątpliwości co do tego, iż za robakiem *Stuxnet* rzeczywiście stał Izrael oraz Stany Zjednoczone, ponieważ trudno wskazać na jakiekolwiek inne państwo, które zarazem miałoby odpowiedni potencjał technologiczny i ekspercki w tej dziedzinie, jak i wyraźny motyw. Podobny program być może mogły stworzyć Chiny oraz Rosja, które jednak nie miały w tym żadnego interesu. Z kolei inne kraje, które mogły chcieć zatrzymać proces wzbogacania uranu przez reżim ajatollahów, takie jak np. Egipt czy Arabia Saudyjska, nie byłyby w stanie przygotować tak skomplikowanego i zarazem skutecznego kodu.

Omówiony wyżej robak okazał się tylko pierwszym z całej serii niezwykle zaawansowanych złośliwych programów, które odkryto w kolejnych latach. Już

[172] *'Israel tested Stuxnet virus on Dimona plant'*. „The Jerusalem Post" 16.01.2011: www.jpost.com/Iranian-Threat/News/Israel-tested-Stuxnet-virus-on-Dimona-plant; dostęp: 27.01.2014.

[173] *Snowden confirms NSA created Stuxned with Israeli aid*. RT.com, 11.07.2013: http://rt.com/news/snowden-nsa-interview-surveillance-831; dostęp: 27.01.2014.

[174] J. Markoff, D.E. Sanger: *In a Computer Worm, a Possible Biblical Clue*. „The New York Times" 29.09.2010: www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&_r=0; dostęp: 29.01.2014.

w październiku 2011 roku zespół węgierskich informatyków z Budapest University of Technology and Economics odkrył *Duqu*, nowy typ złośliwego oprogramowania oparty na technologii oraz kodzie *Stuxnetu*. W przygotowanym przez nich 60-stronicowym raporcie podkreślono, że jest to program oparty w dużej mierze na rozwiązaniach wcześniej odkrytego robaka (wykorzystanie serwerów C&C czy podrobionych certyfikatów bezpieczeństwa), choć *de facto* pełnił nieco inne funkcje. Posiadał m.in. zdolności *keyloggera*, czyli aplikacji rejestrującej każdą aktywność użytkownika na komputerze. Nadano mu nazwę *Duqu* ze względu na tworzony przez niego plik .DQ (Bencsáth, Pék, Buttyán, Félegyházi, 2011). W wyniku tej publikacji społeczność naukowa oraz eksperci podjęli szeroko zakrojone wysiłki na rzecz jego głębszego zbadania. Były one utrudnione nie tylko ze względu na poziom jego skomplikowania, ale także wykorzystanie trudnego do zidentyfikowania języka programowania[175]. Niemniej stosunkowo szybko pojawiły się kolejne raporty wyjaśniające główne cechy i funkcje nowego *malware*. Przede wszystkim stwierdzono, iż nie był on rozpowszechniony na taką skalę jak jego poprzednik. Mimo to był w stanie zainfekować komputery w 8 krajach, w tym m.in. w Iranie, Indiach oraz Francji. Według ocen ekspertów korporacji Symantec prawdopodobnie użyto go już w listopadzie 2010 roku, choć pierwsze ślady jego aktywności pojawiły się w kwietniu 2011 roku. Później co jakiś czas jego twórcy przygotowywali kolejne, zaktualizowane warianty programu[176]. Wśród najważniejszych właściwości *Duqu* specjaliści McAfee Labs wymienili m.in.: podobieństwo do struktury *Stuxnetu*, brak zdolności ataku na systemy przemysłowe typu SCADA/ICS, infekowanie za pomocą złośliwego pliku Microsoft Word wykorzystującego *exploit* dnia zerowego, zarażenie ograniczonej liczby podmiotów, posiadanie podrobionych certyfikatów cyfrowych, samoistnie usuwanie się z komputera po 30 lub 36 dniach od zarażenia. Ponadto dodali, iż *Duqu* nie był wymierzony w instalacje sektora energetycznego, a jego serwery kontrolujące znajdowały się w Belgii oraz Indiach (*Duqu*, 2011).

Na tej podstawie zaliczono go do grupy trojanów, jego główną funkcją było bowiem pozyskiwanie niejawnych danych w formie cyfrowej, na co zresztą wskazywały zaawansowane zdolności w tym zakresie. Należy tu wymienić m.in. możliwość zapamiętywania aktywności użytkownika na danym komputerze (w tym wszystkich wciśniętych klawiszy), zdobywania informacji o danej jednostce (wersja systemu operacyjnego wraz z aktualizacjami, nazwa komputera, użytkownicy), listach procesów, aktywnych połączeniach sieciowych, udostępnianych folderach, a także o wszystkich podłączonych maszynach i urządzeniach. Administrator *Duqu* miał także możliwość tworzenia zrzutów z ekranu

[175] I. Soumenkov: *The Mystery of the Duqu Framework*. SecureList, 07.03.2012: www.securelist.com/en/blog/667/The_Mystery_of_the_Duqu_Framework; dostęp: 29.01.2014.

[176] Data kompilacji pierwszego wariantu *Duqu* to 11 marca 2010 roku. Zob. *W32.Duqu*, 2011, s. 2.

zainfekowanego komputera[177]. Ze względu na modularną strukturę oraz stałe połączenie z serwerami C&C mógł on być systematycznie uzupełniany o nowe komponenty, pozwalające np. na przejęcie kontroli nad daną jednostką. Warto w tym miejscu odwołać się do raportu korporacji Symantec (*W32.Duqu*, 2011: 1), którego autorzy w następujący sposób scharakteryzowali funkcje trojana:

> *W32.Duqu* jest zagrożeniem niemal identycznym do *Stuxnetu*, choć z zupełnie innym przeznaczeniem. […] został napisany przez tych samych autorów lub takich, którzy mieli dostęp do kodu źródłowego *Stuxnetu*. […] Przeznaczeniem *Duqu* jest zbieranie danych wywiadowczych […] od takich podmiotów, jak producenci systemów lub infrastruktury przemysłowej […] w celu łatwiejszego przeprowadzenia ataku w przyszłości. […] Atakujący poszukują informacji, takich jak dokumenty projektowe, które mogłyby pomóc przygotować przyszły atak na rozmaite [instalacje — M.L.] przemysłowe.

Innymi słowy program ten miał zbierać informacje o szeroko pojętej infrastrukturze przemysłowej, które następnie mogłyby posłużyć do kolejnych cyberataków powielających metody znane już ze *Stuxnetu*. Nie dziwi więc fakt, iż Larry Constantine w wywiadzie dla „IEEE Spectrum" stwierdził: „jeśli *Stuxnet* mógłby zostać uznany za inteligentną bombę z jasno określonym celem, to *Duqu* w zasadzie jest typem zwiadowczego dronu"[178]. Z uznaniem na temat możliwości trojana wypowiadali się również jego węgierscy odkrywcy. Ich zdaniem można go było przyrównać do swoistego „zestawu lego" w środowisku *malware*, czyli programu złożonego z niewielkich komponentów, mających ściśle określone funkcje (Bencsáth, Pék, Buttyán, Félegyházi, 2012, s. 979). Na tym tle należy podkreślić, iż ponownie jednym z głównych celów nowego programu stał się Iran, który w listopadzie 2011 roku potwierdził, że odnalazł na swoich komputerach *Duqu* i aktywnie go zwalcza[179]. Na jego związek ze *Stuxnetem* wskazywała również wiadomość, iż był on obecny przede wszystkim na komputerach mających związek z programem atomowym[180]. Mimo to nie ujawniono dokładnych technicznych danych dotyczących konsekwencji zainfekowania irańskich systemów teleinformatycznych.

Stosunkowo szybko okazało się, że *Duqu* nie był jedynym „spokrewnionym" ze *Stuxnetem* typem złośliwego oprogramowania, które wykorzystano przeciwko

---

[177] P. Szor: *Duqu — Threat Research and Analysis*. McAfee Labs, s. 16: http://blogs.mcafee.com/wp-content/uploads/2011/10/Duqu1.pdf; dostęp: 29.01.2014.

[178] S. Cherry: *Sons of Stuxnet*. „IEEE Spectrum" 14.12.2011: http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet; dostęp: 29.01.2014.

[179] H. Jaseb: *Iran says has detected Duqu computer virus*. Reuters, 13.11.2011: www.reuters.com/article/2011/11/13/us-iran-computer-duqu-idUSTRE7AC0YP20111113; dostęp: 29.01.2014.

[180] *Iran Admits Nuclear Sites Hit by 'Duqu' Cyberweapon*. FoxNews, 14.11.2011: www.foxnews.com/tech/2011/11/14/iran-admits-nuclear-sites-hit-by-duqu-cyberweapon/; dostęp: 29.01.2014.

reżimowi ajatollahów. Już w maju 2012 roku badacze z irańskiego zespołu CERT, węgierskiego laboratorium CrySys oraz korporacji Kaspersky Lab rozpoczęli analizę nowego rodzaju *malware*. O podjęcie tych prac zwrócił się do nich Międzynarodowy Związek Telekomunikacyjny, który zareagował w ten sposób na informacje o nowym wirusie, który zaraził komputery irańskiego Ministerstwa ds. Ropy Naftowej. Złośliwy kod określono mianem *Worm.W32.Flame*. Wstępne badania wykazały, iż był to wyjątkowo zaawansowany zestaw narzędzi do przeprowadzania cyberataków, o zdecydowanie bardziej kompleksowej strukturze niż *Duqu* czy *Stuxnet*. Świadczył o tym chociażby fakt, iż zajmował on w sumie ok. 20 MB pamięci, co czyniło go wielokrotnie większym od innych programów tego typu. W momencie odkrycia funkcjonował już nieprzerwanie od kilku lat, choć ustalenie precyzyjnej daty okazało się niemożliwe, ponieważ jego twórcy specjalnie zmodyfikowali daty stworzenia poszczególnych plików, tak aby wskazywały one jeszcze na lata 90. XX wieku[181]. Stosunkowo szybko badacze doszli do wniosku, że program ten, podobnie jak poprzednicy, miał budowę modułową, która pozwalała na elastyczne dostosowywanie jego funkcjonalności do potrzeb operatorów. Jak na tej podstawie stwierdzili specjaliści z CrySys, głównym celem *Flame* było zdobywanie informacji z komputerów posiadających system operacyjny Windows, pozyskiwał je jednak w sposób zdecydowanie bardziej zaawansowany niż *Duqu*. Oprócz standardowych możliwości oferowanych przez większość *keyloggerów* (zapis wciśniętych klawiszy, zrzuty z ekranu) oferował on całą gamę innych, bardziej zaawansowanych instrumentów. Należy do nich zaliczyć m.in.: zdolność włączenia nieaktywnych kamer oraz mikrofonów komputerowych, nagrywanie za ich pomocą dźwięków i obrazów z otoczenia, przeglądanie pamięci przenośnej, podłączonej do danej jednostki czy wykorzystanie technologii Bluetooth do przesyłania informacji o zaatakowanym systemie (Bencsáth, Pék, Buttyán, Félegyházi, 2012, s. 980).

Warto również przywołać opinię irańskiego zespołu CERT, który wyróżnił szereg podstawowych cech charakterystycznych *Flame'a*: rozpowszechniał się za pomocą nośników pamięci (np. USB) oraz sieci lokalnych, dokonywał tzw. *network sniffingu*, czyli analizy ruchu w danej sieci, kompletował listy wrażliwych haseł, skanował dyski twarde w poszukiwaniu określonych rozszerzeń lub danych, automatycznie dokonywał zrzutów z ekranu w z góry przewidzianych okolicznościach, mógł przejmować kontrolę nad mikrofonami podłączonymi do komputera, przesyłał zdobyte dane do serwerów dowodzenia i kontroli (C&C), tworzył bezpieczne połączenia z serwerami C&C za pomocą protokołów SHH i HTTPS, skutecznie omijał zabezpieczenia wprowadzone przez najbar-

[181] Przy czym zdaniem węgierskich naukowców okres jego funkcjonowania oscylował w granicach 5—8 lat. Zob. *Analysis Report*, 2012, s. 1; A. Gostev: *The Flame: Questions and Answers.* SecureList, 28.05.2012: www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers; dostęp: 29.01.2014; *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware* 2012, s. 2.

dziej znane programy antywirusowe, infekował systemy Windows 7, Windows XP oraz Windows Vista[182]. Posiadał on zatem bardzo szeroką gamę zdolności przydatnych do skutecznego zbierania informacji o danej organizacji. Nie tylko umożliwiał śledzenie działań użytkownika online, ale dawał także możliwość podsłuchiwania jego rozmów, kopiowania danych z twardego dysku i nośników pamięci oraz innych urządzeń podłączonych do komputera za pomocą technologii Bluetooth (czyli np. z telefonów komórkowych). Kiedy kontrolujący go administratorzy zdobywali wszystkie potrzebne dane, *Flame* sam się usuwał z HDD[183]. Nie dziwi więc fakt, iż wielu badaczy uznawało go wówczas za najbardziej zaawansowany złośliwy program, jaki został dotychczas stworzony[184]. Według ekspertów z Kaspersky Lab autorzy tego trojana wykazywali szczególne zainteresowanie plikami w formacie .PDF, .DOC/DOCX (Microsoft Office) oraz rysunkami technicznymi z programu AutoCad. Eksperci zbadali ponadto infrastrukturę serwerów C&C, które były wykorzystywane do jego kontrolowania. Jak się okazało, istniała ona od lat i obejmowała ponad 80 domen ulokowanych m.in. w Hong Kongu, Turcji, RFN, Polsce, Malezji czy Wielkiej Brytanii[185]. Był to więc wyjątkowo kompleksowy program, który wykorzystywał 5 różnych technik szyfrowania, 3 metody kompresji oraz 5 formatów plików (*sKyWIper*, 2012: 7).

Najważniejsze z perspektywy omawianego tematu jest jednak to, że trojan *Flame* został wykorzystany prawdopodobnie również do zaatakowania irańskiej infrastruktury teleinformatycznej[186]. W kwietniu 2012 roku jego ofiarą padły komputery w Ministerstwie ds. Ropy Naftowej oraz inne instalacje i podmioty związane z sektorem energetycznym[187]. Pojawiły się wówczas informacje o odcięciu sześciu irańskich terminali naftowych od Internetu, co miało być reakcją na powtarzające się cyberataki polegające m.in. na usuwaniu zawartości twardych dysków w komputerach ministerstwa. Warto dodać, że tylko jeden

[182] *Identification of a New Targeted Cyber-Attack*. Iran National CERT (MAHER), 28.05.2012: www.certcc.ir/index.php?name=news&file=article&sid=1894; dostęp: 29.01.2014.

[183] *First Stuxnet — Now the Flame Virus*. The Availability Digest, June 2012: www.availabilitydigest.com/public_articles/0706/flame_virus.pdf; dostęp: 30.01.2014.

[184] K.F. Morton, D. Grace: *A case study on Stuxnet and Flame Malware*. Vixra.org: http://vixra.org/pdf/1209.0040v1.pdf; dostęp: 30.01.2014.

[185] *Kaspersky Lab Experts Provide In-Depth Analysis of Flame C&C Infrastructure*. Kaspersky Lab, 04.06.2012: www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_Experts_Provide_In_Depth_Analysis_of_Flames_Infrastructure; dostęp: 30.01.2014.

[186] Choć trzeba podkreślić, iż zainfekował również inne komputery m.in. na całym Bliskim Wschodzie. Zob. *A New Era of Cyber Warfare*, 2012, s. 3; D. Lee: *Flame: Massive cyber-attack discovered, reserchers say*. BBC News, 28.05.2012: www.bbc.co.uk/news/technology-18238326; dostęp: 30.01.2014.

[187] Warto jednak zauważyć, iż istnieją różne teorie w tej sprawie. Według części ekspertów za usunięcie danych z komputerów irańskiego przemysłu naftowego odpowiadał inny, nieodnaleziony program (*Wiper*), a *Flame* wykorzystywano przede wszystkim do działań cyberszpiegowskich. Zob. A. Gostev: *The Flame*…, op.cit.

z tych terminali, na wyspie Kharg, był odpowiedzialny za przetwarzanie ok. 90% krajowej ropy naftowej, co świadczyło o skali zagrożenia ze strony *Flame'a*. W wyniku tych wydarzeń przestały działać również strony internetowe kilku związanych z nim instytucji, w tym National Iranian Oil Company odpowiedzialnej za sprzedaż ropy naftowej. Wśród innych zaatakowanych podmiotów znalazły się spółki córki NIOC: National Iranian Oil Processing and Distribution Company, National Iranian Gas Company, Iranian Offshore Oil Company, Pars Oil and Gas. Incydenty nie doprowadziły jednak do nieodwracalnych strat, głównie ze względu na fakt, iż sektor ten tylko w niewielkim stopniu zaadaptował najnowsze technologie informacyjne i komunikacyjne, opierał się natomiast nadal na urządzeniach i metodach nieskomputeryzowanych. Nie doszło także do zakłócenia sprzedaży irańskiej ropy na światowych rynkach[188]. Niemniej likwidacja skutków tego cyberataku zajęła odpowiednim służbom aż około miesiąca. Dopiero pod koniec maja pojawiła się w mediach wypowiedź Gholama Rezy Jalalego, według którego program został wykryty i unieszkodliwiony, a utracone dane odzyskane[189].

W październiku 2012 roku Kaspersky Lab ogłosiło odkrycie kolejnego programu szpiegowskiego, niejako wbudowanego we *Flame'a — miniFlame*. Eksperci doszli do wniosku, iż był to niezależny trojan, który mógł pracować zarówno autonomicznie, jak i w charakterze komponentu innych złośliwych programów z szeroko pojętej rodziny *Stuxnet* (*Flame'a* lub późniejszego *Gaussa*). Był on wykorzystywany do pozyskiwania zdalnego dostępu do zasobów komputerowych, choć na zdecydowanie mniejszą skalę niż inne programy z tej grupy, zainfekował bowiem tylko ok. 50—60 komputerów na całym świecie[190].

Ujawnione wówczas informacje były interesujące z kilku powodów. Po pierwsze ponownie rozpoczęła się debata na temat tego, kto stworzył *Flame'a*. Początkowo pojawiły się tutaj pewne kontrowersje związane głównie z raportem badaczy z Budapest University of Technology and Economics. Ich zdaniem pod względem rozwiązań technicznych *Flame* nie czerpał już bowiem z dorobku kodu *Stuxnetu*, wprowadzając zupełnie nowe rozwiązania. Zasugerowali oni, że *Flame* został opracowany przez inny zespół informatyków, przy czym zaznaczyli, iż został on dostosowany do tych samych wymagań opera-

[188] T. Erdbrink: *Facing Cyberattack, Iranian Officials Disconnected Some Oil Terminals from Internet*. „The New York Times" 23.04.2012: www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0; dostęp: 30.01.2014.

[189] *Iran: Powerful „Flame" computer virus briefly hit oil industry but was defeated with data recovered*. CBSNews, 30.05.2012: www.cbsnews.com/news/iran-powerful-flame-computer-virus-briefly-hit-oil-industry-but-was-defeated-with-data-recovered; dostęp: 30.10.2014; N. Hopkins: *Cyber attack on Iranian oil ministry is 'most sophisticated' computer worm yet*. „The Guardian" 28.05.2012: www.rawstory.com/rs/2012/05/28/cyber-attack-on-iranian-oil-ministry-is-most-sophisticated-computer-worm-yet; dostęp: 30.01.2014.

[190] *miniFlame aka SPE: „Elvis and his friends"*. SecureList, 15.10.2012: www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends; dostęp: 31.01.2014.

cyjnych co wcześniejszy *Duqu* (*sKyWIper*, 2012: 7). Wątpliwości w tej kwestii rozwiali dopiero badacze z Kaspersky Lab, którzy jednoznacznie stwierdzili, że *Flame* oraz *Stuxnet* zostały przygotowane przez tych samych autorów. Jako dowód podali fakt, iż jeden z modułów *Stuxnetu* był również istotnym komponentem nowszego trojana (tzw. Resource 207)[191]. Od tego momentu zaczęto akceptować tezę, iż za tymi incydentami po raz kolejny stały służby Izraela oraz Stanów Zjednoczonych[192]. Było to tym bardziej ewidentne, iż zdaniem analityków tak skomplikowanego złośliwego programu nie byłby w stanie stworzyć żaden podmiot pozapaństwowy[193]. Po drugie należy zgodzić się z opiniami ekspertów, którzy zaczęli wówczas sugerować, iż odkrycie trojana *Flame* oznaczało otwarcie nowej fazy cyberwojny między Izraelem i Stanami Zjednoczonymi a Iranem[194], wskazywały na to nawet oficjalne wypowiedzi. Jeden z irańskich polityków Hamidreza Taraghi stwierdził, iż była to kolejna próba prowadzenia „miękkiej wojny" przez Zachód przeciwko Teheranowi, natomiast Mohammed Reza Sabzalipour, szef Tehran World Trade Center, zauważył, że Iran znajduje się w stanie „bezkrwawej wojny", która w przypadku fiaska rokowań atomowych uległaby dalszej intensyfikacji[195]. Z drugiej strony od cyberataków nie odciął się wyraźnie Izrael: wicepremier Moshe Yaalon zapytany przez dziennikarzy o komentarz w tej sprawie odpowiedział, iż każdy, kto postrzega Iran jako poważne zagrożenie, będzie podejmował kroki w celu jego zniwelowania. Dodał przy tym: „Izrael jest pobłogosławiony, będąc krajem bogatym w zaawansowaną technologię. Te instrumenty, z których jesteśmy dumni, otwierają przed nami różne możliwości"[196]. Tym samym dał do zrozumienia, iż to Tel Awiw odpowiadał za te incydenty. Powstaje pyta-

[191] *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected*. Kaspersky Lab, 11.06.2012: www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected; dostęp: 30.01.2014.

[192] E. Nakashima, G. Miller, J. Tate: *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*. „The Washington Post" 19.06.2012: www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html; dostęp: 30.01.2014.

[193] N. Hopkins: *Cyber attack on Iranian oil ministry is 'most sophisticated' computer worm yet*. „The Guardian" 28.05.2012: www.rawstory.com/rs/2012/05/28/cyber-attack-on-iranian-oil-ministry-is-most-sophisticated-computer-worm-yet; dostęp: 30.01.2014.

[194] Tego typu sugestie wyrażał m.in. Eugene Kaspersky. Zob. S. Musil: *Massive cyber-attack dubbed Flame uncovered in Middle East, say researchers*. CBSNews, 28.05.2012: www.cbsnews.com/news/massive-cyber-attack-dubbed-flame-uncovered-in-middle-east-say-researchers; dostęp: 30.01.2014.

[195] T. Erdbrink: *Facing Cyberattack, Iranian Officials Disconnected Some Oil Terminals from Internet*. „The New York Times" 23.04.2012: www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0; dostęp: 30.01.2014.

[196] G. Ronen: *Yaalon Hints Israel behind Flame Malware*. Israel National News, 29.05.2012: www.israelnationalnews.com/News/News.aspx/156294; dostęp: 30.01.2014.

nie, dlaczego właśnie w taki sposób zdecydowano się wykorzystać *Flame'a*. Wcześniej był on używany przez twórców do niewykrywalnych działań cyberszpiegowskich, które przynosiły z pewnością znaczne korzyści. Tymczasem na początku 2012 roku odwołano się do jego specyficznej i pobocznej funkcji, jaką była możliwość skasowania danych na zainfekowanych komputerach. Wywołało to naturalnie reakcję irańskich służb, które nawiązały współpracę z podmiotami zagranicznymi w celu zidentyfikowania oraz usunięcia złośliwego oprogramowania. Jego sygnatury zostały szybko wprowadzone do standardowych programów antywirusowych, a co za tym idzie *Flame* stał się bezużyteczny dla kolejnych akcji cyberszpiegowskich. Oznaczało to więc utratę przez Izrael oraz USA wyjątkowego w swojej istocie narzędzia ofensywnych działań w przestrzeni teleinformatycznej. Ruch ten, jeśli odrzucimy ewentualne nieracjonalne przesłanki, mógł być tłumaczony tylko na trzy sposoby. Być może miał być to test skuteczności cyberataku na infrastrukturę sektora energetycznego Iranu. Ponadto ze względu na jego znaczenie dla irańskiej gospodarki, szczególnie w okresie narastających sankcji społeczności międzynarodowej[197], mogła to być próba wywarcia dodatkowego nacisku na władze w Teheranie przed kolejną rundą negocjacji w sprawie programu atomowego, która miała się odbyć 23 maja 2012 roku. W ten sposób zdarzenia te interpretował wspomniany już Mohammed Reza Sabzalipour[198]. Jeśli rzeczywiście takie były motywy sprawców, to należy stwierdzić, iż nie wpłynęło to w żaden sposób na postawę reżimu ajatollahów[199]. Mogła to być również próba zablokowania sprzedaży irańskiej ropy naftowej.

Bez względu na bezpośredni powód uzasadnione wydaje się przypuszczenie, iż oba państwa zdecydowały się na taki ruch, ponieważ posiadały już inny, bardziej zaawansowany kod tego typu. Trudno bowiem było oczekiwać, że nie przewidywano w przyszłości potrzeby dokonywania innych ataków cyberszpiegowskich mających na celu uzyskanie wrażliwych danych z irańskich systemów teleinformatycznych. Było to tym bardziej ewidentne, iż, jak twierdzili przedstawiciele amerykańskiego wywiadu, *Flame* był narzędziem przydatnym do przygotowywania kolejnych włamań przeciwko elementom infrastruktury krytycznej[200]. Taka interpretacja potwierdziła się już w czerwcu 2012 roku, kiedy odkryto kolejny złośliwy program z rodziny *Stuxnet — Gauss*. Został on zidentyfikowany przez Kaspersky Lab w rezultacie pogłębionych badań nad *Flame'em*. Znając jego zasady działania, eksperci zidentyfikowali kolejny podobny *mal-*

[197] *Q&A: Iran Sanctions*. BBC News, 20.01.2014: www.bbc.co.uk/news/world-middle-east-15983302; dostęp: 30.01.2014.

[198] T. Erdbrink: *Facing Cyberattack, Iranian Officials Disconnected*..., op.cit.

[199] S. Erlanger, R. Gladstone: *Iran Nuclear Talks End with No Deal*. „The New York Times" 24.05.2012: www.nytimes.com/2012/05/25/world/middleeast/iran-nuclear-talks-are-extended-into-second-day.html?pagewanted=all; dostęp: 30.01.2014.

[200] E. Nakashima, G. Miller, J. Tate: *U.S., Israel developed Flame computer virus*…, op.cit.

ware tego typu. Według analizy przeprowadzonej przez tę korporację zaczął on działać już we wrześniu 2011 roku. Tylko od maja 2012 roku zaraził ok. 2500 komputerów na Bliskim Wschodzie. Podobnie jak poprzednicy *Gauss* został zaprojektowany jako program szpiegowski, którego głównym zadaniem było przekazywanie operatorom istotnych informacji na temat zainfekowanych komputerów, w tym historii przeglądarki internetowej, plików *cookies*, haseł czy konfiguracji systemu operacyjnego. Co ciekawe, posiadał wyjątkową i wcześniej niespotykaną zdolność, jaką było wykradanie danych użytkowników bankowości elektronicznej, w tym np. serwisu PayPal czy Citibank. Ponadto tym razem nie został on napisany z myślą o Iranie, lecz o innym państwie: Libanie, z którym Izrael utrzymywał tradycyjnie napięte stosunki. Jak wskazali eksperci Kaspersky Lab, *Gauss* został napisany w taki sposób, aby atakować usługi e-bankowości w tym kraju. Działania te objęły m.in. Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank czy Credit Libanais[201]. Udowodniło to, że Izrael nie ograniczał swojej ofensywnej aktywności w cyberprzestrzeni jedynie do Iranu, jak bowiem trafnie zauważono w raporcie Kaspersky Lab: „odkrycie *Gaussa* wskazuje, że prawdopodobnie istnieje wiele innych związanych [z nim — M.L.] działających złośliwych programów cyberszpiegowskich. Obecne napięcia na Bliskim Wschodzie są jedynie znakiem intensywności tych trwających kampanii cyberwojennych i cyberszpiegowskich" (*Gauss* 2012: 48). Należy zgodzić się z tym stwierdzeniem, ponieważ jeśli izraelskie i/lub amerykańskie służby znalazły czas, aby przygotować program przeznaczony głównie do ataku na libańską bankowość elektroniczną, co z perspektywy interesów narodowych nie miało większego znaczenia, to trudno oczekiwać, aby równolegle nie opracowano innych, mających odmienne przeznaczenie instrumentów cyberataków.

Wszystkie opisane wyżej działania spełniają warunki uznania ich za akty cyberterroryzmu lub cyberszpiegostwa. Ze względu na ich długotrwały charakter mogą być sklasyfikowane jako wyraźny przejaw cyberwojny, ponieważ Izrael oraz Stany Zjednoczone w sposób masowy i powtarzalny przez kilka lat atakowały irańskie sieci i systemy teleinformatyczne z zamiarem bezpośredniego zaszkodzenia infrastrukturze krytycznej państwa (Lewis, 2011: 2). Miało to zatem negatywne skutki dla bezpieczeństwa narodowego Iranu. Szkody okazały się tak duże, iż wymusiły na jego władzach dynamiczny rozwój własnych zdolności ofensywnych i defensywnych w cyberprzestrzeni, rozpoczęto bowiem prace nad kompleksową strategią bezpieczeństwa teleinformatycznego oraz stworzeniem pierwszych wyspecjalizowanych oddziałów wojskowych do walki w tym środowisku. W 2010 roku powstało irańskie Dowództwo Cyberobrony (Gharargah-e

[201] *Kaspersky Lab Discovers 'Gauss' — A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts*. Kaspersky Lab, 09.08.2012: www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts; dostęp: 30.01.2014.

Defa-e Saiberi)[202], w dwa lata później Gholam Reza Jalali ogłosił gotowość operacyjną pierwszych jednostek tego typu[203]. Ponadto doświadczenia te doprowadziły do uwzględnienia zdolności do prowadzenia walki w cyberprzestrzeni w doktrynie wojny asymetrycznej. W konsekwencji już od mniej więcej 2011 roku sam Teheran dokonał kilku poważniejszych cyberataków. Za Gabi Sibonim (2012) można tu wymienić m.in. włamanie do komputerów DigiNotar w Holandii w sierpniu 2011 roku czy instytucji finansowych w USA (Bank of America, Morgan Chase, CitiGroup) we wrześniu 2012 roku. W sierpniu tego roku irański wirus *Shamoon* zainfekował komputery saudyjskiej korporacji energetycznej Aramco, kasując dane w sumie z ok. 30 000 komputerów[204]. W ten sposób nie tylko osłabiono pozycję największego bliskowschodniego rywala Iranu na rynkach energetycznych, ale także zagrożono bezpieczeństwu Stanów Zjednoczonych, częściowo uzależnionych od saudyjskich dostaw[205]. O rosnących zdolnościach Iranu do działań w cyberprzestrzeni świadczyło również przejęcie przez niego kontroli nad amerykańskim dronem zwiadowczym RQ-170 *Sentinel* w grudniu 2011 roku (Heintschel von Heinegg, 2012: 13). W 2012 roku wykryto trojana *Mahdi*, który do lipca zainfekował kilkadziesiąt komputerów w samym Izraelu. Mimo stosunkowo niskiego stopnia zaawansowania technicznego twórcom złośliwego programu udało się jednak wyprowadzić w ten sposób informacje dotyczące funkcjonowania elementów infrastruktury krytycznej tego kraju[206]. Aktywność irańska będąca odpowiedzią na omówione wyżej ataki zwróciła w końcu uwagę amerykańskiej administracji. Sekretarz obrony Stanów Zjednoczonych Leon Panetta w październiku 2012 roku zauważył wzrost zagrożenia w cyberprzestrzeni ze strony Teheranu oraz zadeklarował gotowość do podjęcia działań odwetowych w razie cyberataku wymierzonego w USA[207].

---

[202] H. Bastani: *Structure of Iran's Cyber Warfare*. Institut Français d'Analyse Stratégique, 13.12.2012: www.strato-analyse.org/fr/spip.php?article223; dostęp: 31.01.2014.

[203] *General Jalali: „Iran has begun to operate its first cyber army"*. IranPolitik, 21.02.2012: www.iranpolitik.com/2012/02/21/news/general-jalali-iran-begun-operate-cyber-army; dostęp: 31.01.2014.

[204] T. Shanker, D.E. Sanger: *U.S. Suspects Iran Was Behind a Wave of Cyberattacks*. „The New York Times" 13.10.2012: www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?_r=0; dostęp: 31.01.2014.

[205] C. Krauss: *U.S. Reliance on Oil From Saudi Arabia is Growing Again*. „The New York Times" 16.08.2012: www.nytimes.com/2012/08/17/business/energy-environment/us-reliance-on-saudi-oil-is-growing-again.html; dostęp: 31.01.2014.

[206] Zob. Y. Lappin: *'Mahdi' virus stole data on national infrastructure*. „The Jerusalem Post" 19.07.2012: www.jpost.com/Defense/Mahdi-virus-stole-data-on-national-infrastructure; dostęp: 11.04.2014; K. Zetter: *Mahdi, the Messiah, Found Infecting Systems in Iran, Israel*. „Wired" 17.07.2012: www.wired.com/2012/07/mahdi; dostęp: 11.04.2014; *Cyber-espionage Mahdi virus spreads further in Middle East*. InfoSecurity, 30.08.2012: www.infosecurity-magazine.com/view/27904/cyberespionage-mahdi-virus-spreads-further-in-middle-east; dostęp: 11.04.2014.

[207] *Defense Secretary Leon Panetta: Cyberthreat from Iran has grown*. „Daily News" 12.10.2012: www.nydailynews.com/news/world/panetta-iran-cyberthreat-article-1.1181748; dostęp: 31.01.2014.

Należy podkreślić, iż był to jeden z pierwszych przypadków, w których doszło do tak wyraźnej eskalacji rywalizacji państw w cyberprzestrzeni. W Estonii, Gruzji oraz Syrii wyraźnie dominowała tylko jedna strona, wykorzystując swoją znaczną przewagę technologiczną nad przeciwnikiem, tymczasem Iran zareagował na problemy w swoich systemach teleinformatycznych wyjątkowo szybko, dokonując serii poważnych kontrataków.

Oczywiście kluczową rolę w tych wydarzeniach odegrała rodzina unikalnych złośliwych programów komputerowych zapoczątkowanych przez *Stuxnet*. W pewnym sensie rzeczywiście można było je określić mianem pierwszych „cyberbroni", gdyż poziom ich zaawansowania, a także skuteczność w realizacji wyznaczonych celów były wyjątkowe. Jak podkreślił Maciej Ziarek (2013: 17):

> różnice pomiędzy tradycyjnymi atakami i szkodliwymi programami a zaawansowanymi cyberbroniami są widoczne gołym okiem. […] pierwsza grupa aplikacji ma charakter masowych ataków, których celem są zwykli użytkownicy lub firmy niezwiązane z rządem danego państwa i strategicznymi gałęziami przemysłu. Drugą grupę stanowią cyberbronie, które wymierzone są przeciwko obywatelom oraz agencjom innym państw. Programy te są wysoce zaawansowane i szukają konkretnych informacji. […] odstępstwem od tej reguły wśród cyberbroni okazał się *Stuxnet*, który miał na celu prowadzić sabotaż urządzeń.

Po raz pierwszy w historii cyberatak doprowadził zatem do fizycznych zniszczeń infrastruktury krytycznej państwa na taką skalę. Co prawda przesadzone są opinie przyrównujące *Stuxnet* do „Hiroszimy cyberwojny" (Gross, 2011), z pewnością jednak był to jakościowy przełom w tej dziedzinie (Caplan, 2013: 103—104). Warto przytoczyć w tym kontekście słowa Seana Wattsa, który stwierdził, iż *casus* ten był dowodem na to, że krytyka wobec osób wskazujących na rosnące wyzwania dla bezpieczeństwa teleinformatycznego była nieuzasadniona. Jego zdaniem potwierdziło się wówczas, że włamanie komputerowe może wiązać się ze zniszczeniami materialnymi, a co za tym idzie być interpretowane na gruncie prawa wojny[208]. Jak jednak zauważyli m.in. Oona A. Hathaway, Rebecca Crootof, Philip Levitz czy Haley Nix (2012: 885), obecnie obowiązujące regulacje prawne okazały się niewystarczające w świetle szybko ewoluujących działań w cyberprzestrzeni.

[208] Przy czym należy zauważyć, iż zachodni naukowcy nie zgadzają się jednak w pełni co do fundamentalnego znaczenia incydentów związanych ze *Stuxnetem*. Jakkolwiek większość podkreśla, że stanowił on doniosły przełom, istnieje grupa badaczy, którzy marginalizują znaczenie tych zagadnień. Erik Gartzke (2013: 73) stwierdził na przykład, że znaczenie działań ofensywnych w cyberprzestrzeni jest *de facto* niewielkie. Zob. też Watts, 2012: 244—245.

Wszystkie omówione wyżej incydenty teleinformatyczne bez wątpienia były jednym z najciekawszych przykładów wykorzystania potencjału cyberprzestrzeni do realizacji określonych celów polityki zagranicznej. Ze względu na obiektywne trudności konwencjonalnej reakcji na irański program atomowy w drugiej połowie pierwszej dekady XXI wieku Izrael oraz Stany Zjednoczone podjęły decyzję o wykorzystaniu nowatorskich i wcześniej nie stosowanych na taką skalę środków — złośliwych programów komputerowych. Specyfika sieci komputerowych pozwalała na podjęcie działań, które nie rodziły żadnych konsekwencji prawnych, a jednocześnie pozwalały uzyskać wpływ na tempo procesu wzbogacania uranu przez reżim ajatollahów. W tym kontekście warto zwrócić uwagę na kilka kwestii, istotnych z punktu widzenia postawionego we wstępie celu badawczego. Sabotaż komputerowy zastosowany przez Tel Awiw oraz Waszyngton stał się nie tylko substytutem interwencji wojskowej, lecz również środkiem wywierania dodatkowego nacisku na Teheran, co miało zwiększyć efektywność sankcji gospodarczych i zarazem wzmocnić stanowisko negocjacyjne państw zachodnich. Skuteczność tych metod była różna. W zasadzie największy sukces osiągnął robak *Stuxnet*, który doprowadził do zniszczenia około 1000 wirówek wzbogacających uran, tym samym skutecznie doprowadzając do opóźnień w irańskim programie atomowym. Również programy *Duqu* oraz *Flame* osiągnęły swoje podstawowe założenia, skutecznie infekując komputery znajdujące się w kręgu zainteresowania izraelskiego i amerykańskiego wywiadu i przejmując z nich dane. Zwiększyło to podatność irańskich systemów teleinformatycznych na kolejne włamania. *Flame* został ujawniony niejako na życzenie jego twórców, którzy prawdopodobnie chcieli w ten sposób wywrzeć dodatkowy nacisk na władze w Teheranie przed zbliżającymi się negocjacjami w sprawie programu atomowego. Z jednej strony instrumenty teleinformatyczne wpisały się więc w szerszą gamę środków politycznych, gospodarczych czy wojskowych, stosowanych przez Izrael oraz USA[209], z drugiej nie przyniosło to oczekiwanych skutków w perspektywie krótkoterminowej, ponieważ cyberatak miał wyłącznie charakter doraźny, a nie był dogłębnie przemyślaną i perfekcyjnie zrealizowaną operacją, tak jak w przypadku *Stuxnetu*. Porozumienie w tej sprawie zawarto zatem dopiero w styczniu 2014 roku. W zamian za obietnicę państw E3/EU+3, aby nie nakładać kolejnych sankcji, reżim zgodził się m.in. ograniczyć zapasy wzbogaconego uranu do 20%, zaprzestać większych prac nad budową reaktora w Araku, a także udostępnić swoje ośrodki ekspertom Międzynarodowej Agencji Energii Atomowej (Kulesa, 2014: 1). W tej perspektywie wykorzystanie ataków komputerowych miało więc głównie (choć nie tylko — *Stuxnet*),

[209] Wśród środków wojskowych można wskazać chociażby regularne loty zwiadowcze amerykańskich dronów nad Iranem. Zob. D. Cenciotti: *Iran Seizes A U.S. Stealth Drone By Taking Over Controls. Maybe... And What About That Predator Virus*. „The Aviationist" 04.12.2011: http://theaviationist.com/2011/12/04/iran-drone; dostęp: 31.01.2014.

charakter komplementarny w stosunku do innych metod nacisku na reżim ajatollahów.

Reasumując, na przełomie pierwszej i drugiej dekady XXI wieku cyberprzestrzeń stała się nowym wymiarem rywalizacji i konfrontacji między Izraelem i Stanami Zjednoczonymi a Iranem. Z jednej strony jakościowym przełomem było wykorzystanie przez dwa pierwsze państwa zaawansowanych cyberbroni, które doprowadzając do fizycznych zniszczeń w Natanz, spowolniły irański program atomowy. Tym samym, jak stwierdził Kenneth Geers, udało się osiągnąć cel, którego nie zrealizowały kolejne rezolucje Rady Bezpieczeństwa ONZ (Geers, 2011: 13). Ataki te stanowiły ponadto jeden z wielu środków nacisku na władze w Teheranie, aby ugięły się pod międzynarodową presją. Z drugiej strony reżim ajatollahów nie pozostał dłużny, reagując na nie własnymi działaniami w przestrzeni teleinformatycznej, obliczonymi na ochronę swoich interesów na Bliskim Wschodzie. W tym kontekście, jakkolwiek aktywność tych państw w cyberprzestrzeni nie miała charakteru decydującego, udowodniła, iż zjawisko rywalizacji i konfrontacji państw w tej sferze nie tylko istnieje, ale jego natężenie stale wzrasta.

4.7. Przestrzeń teleinformatyczna jako nowa domena rywalizacji na Półwyspie Koreańskim

Cyberprzestrzeń na początku XXI wieku zaczęła stawać się nową sferą aktywności rządów nie tylko na Bliskim Wschodzie i w przestrzeni poradzieckiej, lecz również w Azji Wschodniej. Znaczną uwagę środowiska naukowego w ostatnich latach przyciągnęły wydarzenia na Półwyspie Koreańskim, podzielonym na dwa wrogie sobie kraje, znajdujące się od dziesięcioleci formalnie w stanie wojny. Wynikało to z faktu, iż obok regularnych kryzysów politycznych czy wojskowych od drugiej połowy pierwszej dekady XXI wieku z coraz większą intensywnością zaczęły występować w stosunkach wewnątrzkoreańskich incydenty teleinformatyczne. Warto podjąć próbę pogłębionej analizy charakteru i znaczenia tych zagadnień.

Na wstępie należałoby odnieść się szerzej do podstawowych uwarunkowań relacji wewnątrzkoreańskich. Oczywiście źródeł podziału Półwyspu Koreańskiego na dwa państwa należy upatrywać w wydarzeniach II wojny światowej. Kiedy 15 sierpnia 1945 roku Japonia poddała się aliantom, Związek Radziecki oraz Stany Zjednoczone uzgodniły podział Korei wzdłuż 38. równoleżnika. Strefa północna wokół Phenianu została zajęta przez ZSRR w sierpniu, tymczasem południowa z Seulem przez USA na początku września. Szybko okazało się, że współpraca obu byłych aliantów w warunkach rozpoczynającej się zimnej

wojny będzie niezwykle trudna. Już w lutym 1946 roku, bez względu na prace wspólnej radziecko-amerykańskiej komisji ds. utworzenia koreańskiego rządu, ZSRR zaczęło budować w Phenianie odrębne, komunistyczne struktury władzy. W efekcie komisja została rozwiązana, a w dwa lata później powstał pierwszy cywilny rząd Korei Południowej. 9 września 1948 roku powstała również Koreańska Republika Ludowo-Demokratyczna. Oba państwa, ogłaszając niepodległość, uznawały się za wyłącznych przedstawicieli Korei, a co za tym idzie rościły sobie prawo do kontroli nad całym Półwyspem. Naturalnie doprowadziło to konfliktu zbrojnego między nimi w latach 1950—1953 (Weathersby, 1993). 27 lipca 1953 roku podpisano porozumienie o zawieszeniu broni, w którego wyniku powstała koreańska strefa zdemilitaryzowana, oddzielająca od tej pory oba państwa (Chang-Il, 2010; *A Comprehensive Resolution*, 2003).

Po zakończeniu konfliktu stosunki wewnątrzkoreańskie nadal były bardzo napięte. Korea Północna utrzymywała bliskie relacje, choć z różnym natężeniem, zarówno z Chińską Republiką Ludową, jak i ze Związkiem Radzieckim. Odgrywała tym samym rolę ważnego instrumentu polityki antyamerykańskiej bloku państw komunistycznych (Kim, 2007: 20). Tymczasem Korea Południowa zacieśniała swoje sojusznicze związki przede wszystkim ze Stanami Zjednoczonymi[210]. Stosunki wewnątrzkoreańskie były zdeterminowane głównie rywalizacją o uznanie na arenie międzynarodowej. Towarzyszyły temu znaczne ograniczenia swobód obywatelskich, nie tylko w części północnej. W efekcie w początkowym okresie zimnej wojny w zasadzie trudno było mówić o jakichkolwiek, nawet ograniczonych relacjach między oboma państwami, nawet w wymiarze czysto personalnym. Występowały natomiast częste incydenty wojskowe na linii demarkacyjnej. W rezultacie do ograniczonego ocieplenia wzajemnych kontaktów doszło naprawdę dopiero na przełomie lat 80. i 90. XX wieku. W 1991 roku nastąpiło zawarcie porozumienia o nieagresji i rekoncyliacji, w 1992 roku przyjęto natomiast wspólną deklarację o denuklearyzacji Półwyspu Koreańskiego (*An Overview of Inter-Korean Relations*, s. 2—3).

W tym przełomowym okresie początku lat 90. XX wieku doszło do znacznego osłabienia Koreańskiej Republiki Ludowo-Demokratycznej. Złożyło się na to kilka czynników. Przede wszystkim wynikało to z doniosłych przemian geopolitycznych na całym świecie, związanych z upadkiem bloku państw komunistycznych i zanikiem układu bipolarnego. W nowej sytuacji Phenian stał się krajem osamotnionym, niemogącym już opierać swojej polityki na współpracy z ZSRR. Było to tym bardziej ewidentne, iż Północ była w ogromnym stopniu zapóźniona zarówno gospodarczo, technologicznie, jak i społecznie w stosunku do Seulu. Co więcej, w takiej sytuacji w oczach wielu rządów

[210] R. Weitz: *From Allies to Partners: South Korea and the United States*. „World Politics Review" 09.07.2013: www.worldpoliticsreview.com/articles/13080/from-allies-to-partners-south-korea-and-the-united-states; dostęp: 1.02.2014.

w Azji Wschodniej KRLD zaczęła być postrzegana jako państwo upadłe lub część „osi zła". Po drugie w Korei Południowej do władzy doszedł nastawiony antykomunistycznie prezydent Kim Young Sam, który nie zamierzał tolerować kolejnych wrogich aktów reżimu Kimów. Po trzecie gwałtownie pogorszyła się sytuacja gospodarcza, co w konsekwencji doprowadziło do klęski głodu w KRLD (Armstrong, 2005; *An Overview of Inter-Korean Relations*, s. 3—4). W związku z tymi niekorzystnymi tendencjami Phenian zaczął przykładać zasadniczą wagę do prowadzonego przez siebie od lat programu atomowego. Na tym tle od 1991 roku dochodziło do coraz większych napięć na linii Korea Północna — MAEA, które doprowadziły także do zaostrzenia stosunków z Koreą Południową oraz Stanami Zjednoczonymi. Mimo ostatecznie zawartego porozumienia, które zapobiegło opuszczeniu przez reżim traktatu NPT, program atomowy KRLD nie został zatrzymany (Nikitin, 2013: 1). Oznaczało to pojawienie się poważnego zagrożenia nie tylko dla bezpieczeństwa Korei Południowej, lecz także Stanów Zjednoczonych i ich pozostałych sojuszników w Azji Wschodniej.

W kolejnych latach stosunki wewnątrzkoreańskie charakteryzowały się naprzemiennymi okresami narastających napięć oraz prób rekoncyliacji. Z jednej strony regularnie podejmowano starania na rzecz zbliżenia, czego symbolem stała się tzw. słoneczna polityka zainicjowana przez nowego przywódcę Korei Południowej Kim Dae Junga pod koniec lat 90. XX wieku (Kim, 2007: 72—75). Mimo zasadniczych przeszkód tego typu inicjatywy były kontynuowane w pierwszej dekadzie XXI wieku i doprowadziły do szczytu międzykoreańskiego w październiku 2007 roku, podczas którego podpisano deklarację o stosunkach dwustronnych, pokoju i dobrobycie (Foster-Carter, 2007). Z drugiej jednak strony należy podkreślić, iż koncyliacyjna wobec Północy polityka Seulu przyniosła bardzo ograniczone efekty, ponieważ Phenian borykający się z coraz większymi problemami wewnętrznymi oraz międzynarodową izolacją nie był zainteresowany trwałym porozumieniem z Południem. Na pogorszenie sytuacji KRLD wpływ miało objęcie władzy przez George'a W. Busha, który zaliczył ją w 2002 roku do tzw. „osi zła", obok Iranu oraz Iraku (Matray, 2013: 140—169). Oczywiście istotną rolę odgrywała także pogłębiająca się przepaść gospodarcza i technologiczna z Południem, napięte relacje z Japonią, a także ochłodzenie stosunków z Chińską Republiką Ludową w połowie pierwszej dekady XXI wieku[211].

W takiej sytuacji, jak słusznie zauważył Samuel S. Kim (2007: 81—85), głównym założeniem północnokoreańskiej polityki zagranicznej było zapewnienie bezpieczeństwa państwa. Aby to osiągnąć, biorąc pod uwagę wszystkie

[211] Chanlett-Avery, Rinehart, 2014, s. 3—4; J. Bajoria, B. Xu: *The China-North Korea Relationship*. Council on Foreign Relations, 21.02.2013: www.cfr.org/china/china-north-korea-relationship/p11097#p2; dostęp: 1.02.2014.

niekorzystne tendencje, Phenian, zdaniem Kima, zaadoptował zaawansowaną strategię działań odwołującą się zarówno do sposobów znanych z konfliktów asymetrycznych, jak i do negocjacji. Główną przesłanką przyjęcia takiego podejścia miało być zredukowanie alternatywnych możliwości działań przeciwnika oraz „osłabienie jego zdecydowania" (Kim, 2007: 81—85). Podstawowym środkiem wykorzystywanym przez reżim Kimów były naturalnie siły zbrojne, których rozwój był zawsze priorytetem. Z jednej strony istotną rolę odgrywało tu wykorzystanie konwencjonalnych sił zbrojnych, które, jakkolwiek zapóźnione technologicznie, utrzymywały wysokie morale oraz samą swoją wielkością stanowiły poważne zagrożenie dla Seulu, który oparł swoją politykę bezpieczeństwa na bliskiej współpracy z USA, obecności wojsk amerykańskich na swoim terytorium oraz rozwoju własnego potencjału militarnego[212]. Z drugiej, jak wspomniano, fundamentalne znaczenie dla Północy zyskał program zdobycia broni atomowej. Ze względu na nieefektywność międzynarodowych prób jego zablokowania doprowadziło to w konsekwencji do spełnienia tych ambicji. Ogłoszono to oficjalnie w lutym 2005 roku. Na potwierdzenie trzeba było zaczekać do 9 października 2006 roku, kiedy przeprowadzono pierwszy próbny wybuch jądrowy. Jak stwierdzono w oficjalnym komunikacie Ministerstwa Spraw Zagranicznych KRLD, broń tego typu miała „służyć jako niezawodny środek odstraszania przed wojną", przede wszystkim w kontekście pogarszających się stosunków z USA (Durkalec, 2007: 363). Towarzyszył temu rozwój programu rakiet balistycznych zarówno krótkiego, jak i dalekiego zasięgu, czego potwierdzeniem były m.in. próby przeprowadzone w lipcu 2006 roku (Haliżak, 2013b: 283).

W związku z tym generalnie polityka Korei Północnej od lat 90. XX wieku charakteryzowała się dwoma pozornie sprzecznymi tendencjami. Jak zauważyli Emma Chanlett-Avery i Ian E. Rinehart, wahała się ona między ograniczoną współpracą ze społecznością międzynarodową a otwartymi prowokacjami, do których należy zaliczyć testy rakiet balistycznych oraz 3 próbne wybuchy jądrowe. Ich zdaniem „gotowość Phenianu do negocjacji często wydawała się uzależniona od czynników wewnętrznych: braki żywności czy desperacja gospodarcza mogą popchnąć Koreę Północną do wznowienia rozmów, z reguły aby uzyskać więcej pomocy z Chin lub, w przeszłości, z Korei Południowej". Zdaniem autorów reżim Kimów umiejętnie potrafił rozgrywać różnice interesów pomiędzy poszczególnymi stronami uczestniczącymi w negocjacjach, a także wykorzystywać momenty zmiany władzy w Waszyngtonie do zablokowania negocjacji nuklearnych (Chanlett-Avery, Rinehart, 2014: 4; Nikitin, 2013). W związku z tym można się więc zgodzić ze stwierdzeniem, iż

[212] S. Seongho: *Inter-Korean Relations without the U.S.-ROK Aliance*. „NBR/KFiS U.S.-ROK Alliance Conference Paper". Seoul 2007, s. 22—23: www.nbr.org/downloads/pdfs/PSA/USROK_Conf07_Sheen.pdf; dostęp: 1.02.2014.

> Korea Północna, jeden z najbardziej totalitarnych reżimów na świecie, prowadzi politykę zagraniczną opartą na szantażu nuklearnym (na przemian wracaniu do programu atomowego i wycofywaniu się z niego), wspartego próbami z rakietami średniego zasięgu. Powszechnie traktowana jako zagrożenie dla pokoju i stabilności, Korea Północna broni się przed sankcjami, korzystając ze wsparcia politycznego Chin i Rosji (Łoś-Nowak, red., 2008: 371).

Jak wspomniano wyżej, w praktyce tendencje te w stosunkach wewnątrzkoreańskich przejawiały się regularnymi incydentami zarówno o charakterze politycznym, jak i wojskowym. Do pierwszego, wspomnianego już, doszło na początku lat 90. XX wieku, kiedy Korea Północna zagroziła wycofaniem się z traktatu NPT (Kim, 2007: 84—86). Następny miał miejsce w 1996 roku, kiedy odkryto przy Gangneung północnokoreański szpiegowski okręt podwodny, który utknął na mieliźnie. Znajdujący się na nim agenci wywiadu KRLD uciekli w pobliskie góry, gdzie przez ponad 50 dni poszukiwało ich ok. 60 000 żołnierzy z Południa[213]. Do kolejnego podobnego wydarzenia doszło w dwa lata później, kiedy odkryto następny szpiegowski okręt podwodny przy wybrzeżu (Kirk, 1998). Wzrost napięcia odnotowano także w 1999 roku, kiedy z winy Korei Północnej doszło do bitwy morskiej niedaleko Yeonpyeong, w której wyniku zginęło kilkudziesięciu marynarzy KRLD. Nie zakończyło to jednak bynajmniej prowokacji, granica była bowiem naruszana w 1999 roku w sumie ok. 70 razy. Warto dodać, że w tym samym miejscu doszło do starć jeszcze w 2002 i 2004 roku. Po kilkuletniej przerwie kolejne incydenty nastąpiły w 2009 roku, kiedy doszło do serii prowokacji wojskowych oraz ostrych wypowiedzi przedstawicieli KRLD wobec Korei Południowej. Między styczniem a marcem wystrzelono np. ok. 1000 pocisków artyleryjskich w kierunku wysp sąsiada. W kolejnych miesiącach dochodziło także do przekraczania granicy morskiej przez okręty wojenne Phenianu. Mimo sygnałów chęci polepszenia stosunków dwustronnych przez reżim Kimów prowokacje kontynuowano. Skutkiem tego była bitwa, która miała miejsce w listopadzie w okolicach wyspy Teach'ong. Kryzys sięgnął zenitu w 2010 roku, kiedy południowokoreański okręt Ch'onan został zatopiony torpedą wystrzeloną przez jednostkę KRLD. Niedługo później doszło także do ostrzału artyleryjskiego wyspy Yeonpyeong (zob. *North Korea*, 2010). Wszystkie te wydarzenia jasno potwierdzały przywołane wyżej opinie wskazujące na tendencję do wykorzystania potencjału wojskowego jako środka nacisku nie tylko na władze Korei Południowej, lecz także resztę społeczności międzynarodowej. Wraz z szantażem nuklearnym tego typu działania, stanowiące *de facto* agresję zbrojną, miały wymusić na Seulu czy Waszyngtonie korzystne dla Phenianu decyzje dotyczące m.in. udzielenia pomocy gospodarczej i humanitar-

[213] *DMZ Flashpoints: The 1996 Spy Submarine Incident*. ROK Drop, 14.01.2009: http://rokdrop.com/2009/01/14/nk-spy-submarine-incident-in-gangneung; dostęp: 1.02.2014.

nej. Było to tym wyraźniejsze, iż takie prowokacyjne gesty miały z czasem coraz mniejszą skuteczność[214].

W tym kontekście w stosunkach wewnątrzkoreańskich rosnące znaczenie zaczęły zyskiwać najnowsze technologie teleinformatyczne. Na pozór takie tendencje wydawały się mało realne. Wynikało to z faktu, iż oba państwa dzieliła przepaść, jeśli chodzi o stopień rozwoju społeczeństwa informacyjnego czy procesów komputeryzacji i informatyzacji. Na początku XXI wieku Korea Południowa znalazła się w czołówce najbardziej zaawansowanych technologicznie państw świata. Świadczył o tym przytaczany już *ICT Development Index* Międzynarodowego Związku Telekomunikacyjnego, w którym od lat klasyfikowano ten kraj na pierwszym miejscu (*Measuring the Information Society*, 2012: 46). Tak wysoka ocena Seulu wiązała się nie tylko ze znaczną dostępnością Internetu wśród społeczeństwa, ale także takimi kwestiami, jak prowadzenie innowacyjnej polityki w sektorze teleinformatycznym, regulacja rynku telekomunikacyjnego, opracowywanie nowych technologii czy powszechne wykorzystanie ICT w życiu społecznym[215]. Należy podkreślić, że Korea Południowa stała się jednym z największych producentów oprogramowania i sprzętu komputerowego. Specjalizuje się w tym wiele korporacji, w tym np. AhnLab Inc. (oprogramowanie), Cyworld (media społecznościowe), Daum Communications (usługi internetowe), Empas (wyszukiwarki internetowe), INCA Internet (oprogramowanie antywirusowe, zabezpieczenia) czy Penta Security Systems (zabezpieczenia komputerowe)[216]. O zaawansowaniu Korei Południowej najlepiej świadczyły jednak trwające kilkadziesiąt lat wysiłki na rzecz daleko idącej integracji rządu i administracji państwowej z cyberprzestrzenią (e-rząd, e-administracja)[217]. Mimo głębokiego uzależnienia od ICT Seul nie przywiązywał jednak przez lata większej wagi do kwestii bezpieczeństwa teleinformatycznego. W większości zestawień państw o największym potencjale w tej dziedzinie Korea Południowa w ogóle nie figurowała.

Tymczasem zupełnie inna sytuacja miała miejsce w Korei Północnej, która była na początku XXI wieku jednym z najbardziej zapóźnionych technologicznie krajów globu. Świadczyło o tym kilka czynników. Przede wszystkim wynikało to zarówno z poważnych problemów gospodarczych, jak i totalitarnego systemu politycznego. W efekcie nawet najprostsze urządzenia telekomunika-

[214] Zob. J.-S. You: *The Cheonan Dilemma, Inter-Korean Relations, and the Six Party Talks: A Korean Perspective*. University of California: http://irps.ucsd.edu/assets/001/503063.pdf; dostęp: 2.02.2014.

[215] E. Phneah: *ITU: South Korea top ICT nation again*. ZDNet, 12.10.2012: www.zdnet.com/itu-south-korea-top-ict-nation-again-7000005658; dostęp: 2.02.2014.

[216] Zob. *Companies listed in South Korea*. Bloomberg Markets: www.bloomberg.com/markets/companies/country/south-korea; dostęp: 2.02.2014.

[217] S.H. Joon: *E-Government of Korea. Achievements & Tasks*. Informatization Policy: www.eng.nia.or.kr; dostęp: 2.02.2014.

cyjne w KRLD były uznawane za niedostępny luksus. W ten sposób postrzegano np. nie tylko telefony komórkowe, lecz nawet ich wersje stacjonarne[218]. W tym świetle zdecydowanie trudniejszy był dostęp do technologii teleinformatycznych. Według raportu z 2004 roku w Korei Północnej znajdowało się jedynie ok. 100 000 komputerów przeznaczonych do prywatnego użytku, z czego większość odpowiadała technologii rozpowszechnionej na Zachodzie na początku lat 90. XX wieku (klasa procesorów 386) (Billo, Chang, 2004: 84). Władze w Phenianie od lat starały się ponadto utrzymać pełną kontrolę nad zastosowaniem ICT przez obywateli. Przejawiało się to na dwa sposoby: po pierwsze zakupy komputerów na czarnym rynku były surowo karane przez władze[219], po drugie ich szczęśliwi posiadacze nie mieli swobodnego dostępu do Internetu, który wymagał specjalnego zezwolenia. Z reguły otrzymywali je wyłącznie niektórzy członkowie partii komunistycznej[220]. Aby zaspokoić podstawowe potrzeby komunikacji, utworzono ściśle kontrolowany, krajowy intranet o nazwie *Kwangmyong*. Sieć obejmująca całą KRLD została jednak odcięta od Internetu. Warto dodać, iż dostęp do niej nie był bynajmniej powszechny[221]. Ponadto Korea Północna została bardzo późno podłączona do globalnej sieci. Pierwsze przedsiębiorstwo udostępniające usługę internetową poprzez Chiny (Silibank) zaczęło funkcjonować w Phenianie dopiero w 2001 roku[222]. Nie dziwi więc fakt, iż w corocznych zestawieniach *ICT Development Index* Korea Północna nie została w ogóle uwzględniona (*Measuring the Information Society*, 2012: 46). Za symboliczny dowód dobitnie obrazujący skalę odcięcia tego kraju od reszty świata pod względem technologicznym można uznać zdjęcie Ziemi nocą zrobione z orbity przez NASA: północna część Półwyspu Koreańskiego jest na nim niemal zupełnie czarna[223].

Omówione powyżej uwarunkowania pozornie sugerowały, iż cyberprzestrzeń nie powinna odgrywać nawet najmniejszej roli w stosunkach wewnątrzkoreańskich. Seul miał dostęp do najnowszych technologii teleinformatycz-

[218] *North Korea: Two million have mobile phones*. BBC News, 05.08.2013: www.bbc.co.uk/news/blogs-news-from-elsewhere-23579368; dostęp: 2.02.2014.

[219] *Used Desktop Computers 'Selling Like Hotcakes' in North Korea*. Radio Free Asia, 06.08.2013: www.rfa.org/english/news/korea/computers-08062013154931.html; dostęp: 2.02.2014.

[220] *Google's Schmidt Calls on North Korea to End Internet Ban*. Bloomberg Technology, 10.01.2013: www.bloomberg.com/news/2013-01-10/n-korea-anxious-to-improve-relations-with-u-s-richardson-says.html; dostęp: 2.02.2014.

[221] A. Riesman: *Inside the Pocket-Sized, Dystopian Internet of North Korea*. Motherboard, 2013: http://motherboard.vice.com/read/inside-the-pocket-sized-dystopian-internet-of-north-korea--2; dostęp: 2.02.2014.

[222] B. Lintner: *North Korea's IT revolution*. „Asia Times Online" 24.04.2007: http://north-korea.narod.ru/dprk_internet.htm; dostęp: 2.02.2014.

[223] *Earth's City Lights*. NASA: http://visibleearth.nasa.gov/view.php?id=55167; dostęp: 2.02.2014.

nych, które jednak były praktycznie bezużyteczne wobec niemal odciętego od Internetu Phenianu. Północ była więc jedynie w marginalnym stopniu podatna na ataki komputerowe, ponieważ ICT nie były wykorzystywane w sektorach o żywotnym znaczeniu dla bezpieczeństwa narodowego. Wydawałoby się, że Korea Północna nie powinna posiadać żadnych instrumentów, które w jakikolwiek sposób mogłyby zaszkodzić zdecydowanie bardziej zaawansowanym sąsiadom, choć należy podkreślić, iż Korea Południowa ze względu na jej stopień uzależnienia od najnowszych technologii mogła uchodzić za dogodny cel włamań. Była to więc klasyczna sytuacja, którą można było określić mianem paradoksu cyberbezpieczeństwa.

Związane z tym potencjalne korzyści bardzo wcześnie zostały dostrzeżone przez reżim Kim Dzong Ila, już w 1990 roku powołał on bowiem pierwszą agencję (Korea Computer Center — KCC), której celem był rozwój technologii ICT w KRLD. Przeznaczono na ten cel wówczas ok. 530 mln dolarów, co świadczyło o dużym znaczeniu, jakie miały dla władz te zagadnienia. Było to tym bardziej ewidentne, iż na czele KCC stanął najstarszy syn Kim Dzong Ila — Kim Dzong Nam, który wcześniej studiował informatykę w Szwajcarii. Nowy organ nie miał bynajmniej rozwijać cywilnych sieci komputerowych. Na wojskowy charakter działalności centrum wskazywał chociażby fakt, iż w tym samym czasie Kim Dzong Nam był szefem krajowych służb bezpieczeństwa (State Safety and Security Agency), funkcjonowanie centrum wiązało się więc prawdopodobnie z pierwszymi próbami budowania zdolności do walki w tworzącym się dopiero Internecie. Przez wiele lat informacje na ten temat były jednak tajemnicą. Temat ten powrócił dopiero na początku XXI wieku. W 2002 roku Richard Clarke, ówczesny doradca prezydenta George'a W. Busha, stwierdził w trakcie jednego z wystąpień przed Kongresem, że Korea Północna rozwija zdolności prowadzenia ataków w przestrzeni teleinformatycznej[224]. Informacje te w 2004 roku potwierdził minister obrony Korei Południowej, który w wystąpieniu parlamentarnym ujawnił, iż KRLD wyszkoliła jednostkę liczącą ponad 500 hakerów. W jego ocenie już wówczas Phenian osiągnął w tej dziedzinie potencjał porównywalny z wieloma krajami rozwiniętymi. Wynikało to z faktu, iż wszyscy zatrudnieni przez Północ specjaliści przechodzili pięcioletnie studia, których głównym założeniem było przygotowanie ich do penetrowania sieci komputerowych Korei Południowej, Japonii oraz Stanów Zjednoczonych. Oznaczało to więc, iż KRLD jako jedno z pierwszych państw na świecie zwróciła uwagę na przydatność działań w cyberprzestrzeni do realizacji wybranych interesów w środowisku międzynarodowym[225].

[224] *Cyberattack could result in military response*. USA Today, 14.02.2002: http://usatoday30.usatoday.com/tech/news/2002/02/14/cyberterrorism.htm; dostęp: 2.02.2014.

[225] B. Lintner: *North Korea's IT revolution*…, op.cit.

W kilka lat później wiadomości te zostały potwierdzone przez inne doniesienia o północnokoreańskiej jednostce wojskowej nr 121, która miała powstać już w 1998 roku. Jej personel liczył wówczas ok. 1000 ekspertów komputerowych przygotowanych w głównej mierze do ataków na amerykańskie i południowokoreańskie sieci[226]. Jak jednak ocenił Kevin Coleman z DefenseTech, w 2007 roku liczyła ona już ok. 17 000 żołnierzy i miała budżet w granicach 70 mln dolarów. Oznaczało to, że Korea Północna pod względem finansowania zdolności do walki w cyberprzestrzeni znajdowała się wśród 25 czołowych krajów świata. Do głównych założeń funkcjonowania jednostki nr 121 Coleman zaliczył m.in. rozwój potencjału do prowadzenia walki asymetrycznej, wkomponowanie działań ofensywnych w cyberprzestrzeni w strategię wojskową KRLD, wykorzystanie cyberataków jako niewojennego środka osiągania potęgi i wpływu, prowadzenie wywiadu elektronicznego (cyberszpiegostwo), a także ataki na infrastrukturę krytyczną przeciwnika w celu wzbudzenia społecznego fermentu oraz doprowadzenia do strat finansowych[227]. Warto tutaj przytoczyć również słowa Jeffreya Carra, którego zdaniem

> Korea Północna wydała znaczne sumy pieniędzy na [rozwój — M.L] swoich zdolności walki informacyjnej. Wysyła swoich żołnierzy do szkół doskonalących w Indiach i Chinach. […] Północnokoreańscy żołnierze walki informacyjnej są dobrze wyszkoleni […], nie postawiłbym ich na czele żadnej listy, ale też nie na końcu. Myślę, że zajmują solidną pozycję średniego szczebla[228].

Nieco innego zdania był południowokoreański badacz Lee Dong Hoon, który stwierdził, że zdolności KRLD do działań w cyberprzestrzeni należałoby oceniać zdecydowanie wyżej. Według pod tym względem była ona trzecim państwem na świecie, po Stanach Zjednoczonych oraz Rosji, a za rozwój tych zdolności oraz rzeczywiste działania w cyberprzestrzeni było odpowiedzialne powstałe w 2009 roku Główne Biuro Wywiadowcze (Reconnaissance General Bureau) grupujące trzy jednostki przeznaczone do akcji sabotażowo-szpiegowskich w sieci. Dodał przy tym, że siły bezpieczeństwa Korei Południo-

[226] D. Danchev: *North Korea's Cyber Warfare Unit 121*. Mind Steams of Information Security Knowledge, 16.07.2006: http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html; dostęp: 2.02.2014.

[227] Warto zauważyć, że zupełnie inne dane przytoczyli Richard A. Clarke i Robert K. Knake (2010: 19). Według nich na północnokoreańskie zdolności do walki cyberprzestrzennej składały się trzy jednostki: nr 121 licząca ok. 600 specjalistów, nr 204 licząca ok. 100 osób oraz nr 35, najmniejsza z nich, lecz wysoko wyspecjalizowana. Zob. K. Coleman: *Inside DPRK's Unit 121*. DefenseTech, 24.12.2007: http://defensetech.org/2007/12/24/inside-dprks-unit-121; dostęp: 2.02.2014.

[228] D. Danchev, J. Carr: *Q&A of the week: 'The current state of the cyber warfare threat' featuring Jeffrey Carr*. ZDNet, 11.05.2012: www.zdnet.com/blog/security/q-and-ampa-of-the-week-the-current-state-of-the-cyber-warfare-threat-featuring-jeffrey-carr/12066; dostęp: 2.02.2014.

wej miały pod tym względem znaczne zapóźnienia w stosunku do Phenianu[229]. Ten punkt widzenia podzielił również Alexandre Mansourov, który zauważył, że od 2009 roku KRLD znacznie zintensyfikowała prace nad rozwinięciem swoich zdolności w tej dziedzinie. Według niego oznaczało to, iż reżim przygotowywał się do przyszłej cyberwojny. Wyrazem tego miały być coraz częstsze ataki komputerowe o charakterze szpiegowskim[230]. W tym kontekście nie dziwią więc słowa generała armii południowokoreańskiej Bae Deukshina, który zauważył, iż dla KRLD strategiczne znaczenie ma jej jednostka walki teleinformatycznej. Według niego Phenian miał za jej pomocą nie tylko siać społeczny zamęt, lecz także bezpośrednio zagrozić bezpieczeństwu narodowemu najpoważniejszych przeciwników (Feakin, 2012: 74). Należy przy tym dodać, iż armia południowokoreańska dostrzegła te wyzwania i podjęła ograniczone działania zmierzające do zabezpieczenia własnych sieci na przełomie XX i XXI wieku (Billo, Chang, 2004: 79).

Wszystkie omówione powyżej procesy i wydarzenia sprawiły, iż reżim Kimów zdecydował się na wykorzystanie cyberataków jako dodatkowego środka nacisku w stosunkach międzynarodowych. Chronologicznie do pierwszych doszło 4 lipca 2009 roku, w amerykańskie święto niepodległości. Tego dnia nieznani wówczas sprawcy użyli metody DDoS głównie przeciwko rządowym witrynom internetowym Stanów Zjednoczonych, należącym m.in. do Departamentu Stanu oraz Departamentu Bezpieczeństwa Krajowego (Clarke, Knake, 2010: 18). Podobny charakter miały incydenty, które wystąpiły trzy dni później. Wtedy jednak do listy celów dodano amerykańskie instytucje finansowe oraz media, jak również instytucje rządowe oraz sektor biznesowy Korei Południowej. Ostatnia fala ataków nastąpiła 9 i 10 lipca 2009 roku[231]. Wśród zaatakowanych stron w Korei Południowej należy wymienić te należące do Kancelarii Prezydenta, Ministerstwa Obrony, Zgromadzenia Narodowego, banku Shinhan, banku NH, banku Korea Exchange, gazety „Chosun Ilbo", a także popularnego portalu internetowego Naver. Wśród zablokowanych witryn amerykańskich można wymienić Biały Dom, Departament Obrony, Agencję Bezpieczeństwa Narodowego, Departament Skarbu, Secret Service, Departament Transportu, Federalną Komisję Handlu, serwis Amazon, serwis Yahoo, giełdy papierów wartościowych (np. NASDAQ, New York Stock Exchange) oraz media („Washington Post"). Oprócz nich zaatakowano także inne, mniej istotne

[229] C. He-Suk: *'N. Korea has third most powerful cyber war capabilities'*. Asia News Network, 06.07.2012: www.asianewsnet.net/news-31578.html; dostęp: 2.02.2014.

[230] M. Clayton: *In cyberarms race, North Korea emerging as a power, not a pushover*. „The Christian Science Monitor" 21.10.2013: www.alaskadispatch.com/article/20131021/cyberarms-race-north-korea-emerging-power-not-pushover; dostęp: 2.02.2014.

[231] J. Markoff, C. Sang-Hun: *Cyberattacks Jam Government and Commercial Websites in U.S. and South Korea*. „The New York Times" 09.07.2009: www.nytimes.com/2009/07/10/technology/10cyber.html; dostęp: 3.02.2014; Clarke, Knake, 2010: 18.

portale, w tym np. www.ahnlab.com (przedsiębiorstwo zajmujące się zabezpieczeniami komputerowymi), www.altools.com, www.auction.co.kr (serwis aukcyjny), www.chosun.com czy www.site-by-site.com. W sumie wzięto na cel ponad 45 poważniejszych witryn internetowych. Warto dodać, że nie wszystkie ataki się udały: część instytucji była w stanie się przed nimi obronić, pozostałe przestały działać lub funkcjonowały o wiele wolniej raptem przez kilka godzin[232].

Wbrew doniesieniom niektórych mediów cyberataki z lipca 2009 roku nie stanowiły żadnego zagrożenia z punktu widzenia bezpieczeństwa narodowego obu państw. Mimo kilkudniowych prób tylko na krótko udało się zablokować wybrane strony sektora publicznego i prywatnego, co nie doprowadziło jednak do poważniejszych zakłóceń w pracy stojących za nimi instytucji. Cyberatak wykorzystał prostą i popularną metodę *Distributed Denial of Service*, w oparciu o sieć *botnet* liczącą według różnych danych od 30 000 do 166 000 komputerów, zlokalizowanych w 74 krajach. Było to więc niewiele w porównaniu z innymi sieciami tego typu, liczącymi nawet wiele milionów jednostek. W konsekwencji ataki generowały tylko ok. 23 Mb/s. Jak ujawnili analitycy Symantec, do zorganizowania tego prowizorycznego *botnetu* wykorzystano trojan *Dozer* (*Trojan. Dozer*), który rozpowszechniał się za pomocą poczty elektronicznej. Jego specyficzną cechą było to, iż 10 lipca miał się samoistnie usunąć, niszcząc przy tym dane na twardych dyskach zainfekowanych komputerów (m.in. pliki o rozszerzeniu .XML, .XLS, .PPT, .DOC, .PDF czy .CCP). Ponadto na HDD nadpisywał zdanie *Memory of the Independence Day* („Pamięć Dnia Niepodległości). Z jednej strony świadczyło to o próbie zatarcia śladów, tak aby analitycy nie byli w stanie zidentyfikować sprawców, z drugiej jednak strony, jak zauważył Joze Nazario z Arbor Networks, ten rodzaj trojana był oparty na wyjątkowo prostym kodzie[233]. Warto również zauważyć, iż służby południowokoreańskie szybko zablokowały adresy IP serwerów, które rozprowadzały szkodliwe oprogramowanie. Znajdowały się one w Austrii, Gruzji, Niemczech, Korei Południowej oraz w Stanach Zjednoczonych[234]. Wszystkie przytoczone wyżej fakty wskazy-

[232] *Ten Days of Rain*, 2011, s. 15; *Governments hit by cyber attack*. BBC News, 08.07.2009: http://news.bbc.co.uk/2/hi/technology/8139821.stm; dostęp: 3.02.2014; J. Markoff, C. Sang-Hun: *Cyberattacks Jam Government and Commercial Websites*…, op.cit.; M. Weaver: *Cyber attackers target South Korea and US*. „The Guardian" 08.07.2009: www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack; dostep: 3.02.2014.

[233] *Are the 2011 and 2013 South Korean Cyberattacks Related?* „Symantec Security Response" 29.03.2013: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related; dostęp: 3.02.2014; J. Markoff, C. Sang-Hun: *Cyberattacks Jam Government and Commercial Websites*…, op.cit.; E. Mills: *Botnet worm in DOS attacks could wipe data out on infected PCs*. CNet, 10.07.2009: http://news.cnet.com/8301-1009_3-10284281-83.html; dostęp: 3.02.2014; *Ten Days of Rain*…, op.cit., s. 11; Clarke, Knake, 2010: 18.

[234] *North Korea launched cyber attacks, says south*. „The Guardian" 11.07.2009: www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks; dostęp: 3.02.2014.

wały więc jednoznacznie, że sprawcy nie dysponowali ani poważną infrastrukturą teleinformatyczną, ani odpowiednią wiedzą, aby osiągnąć zakładane przez siebie cele.

Powstało więc pytanie, kto stał za tymi incydentami, tym bardziej, iż podobne mogło zorganizować wiele podmiotów pozapaństwowych. Już pierwsze komentarze, które pojawiły się w mediach, mówiły o bezpośredniej odpowiedzialności reżimu Korei Północnej. W kolejnych dniach na związek Phenianu z wydarzeniami z lipca zaczęło wskazywać coraz więcej przesłanek. Po pierwsze odkryto, że *Dozer* wykorzystywał dane pochodzące z przeglądarki internetowej w języku koreańskim. Po drugie zasugerowała to południowokoreańska agencja wywiadowcza (National Intelligence Service), która jeszcze w trakcie trwania ataków wykluczyła odpowiedzialność pojedynczych hakerów. Jej zdaniem sposób organizacji i przeprowadzenia tej kampanii sugerował sprawstwo służb państwowych[235]. Po trzecie można przywołać słowa koreańskiego eksperta Hong Hyuna Ika z ośrodka badawczego Sejong Institute, który stwierdził, iż za tymi wydarzeniami stały albo Korea Północna, albo Chiny. Dodał przy tym, że już od lat Phenian starał się uzyskać dostęp do południowokoreańskich sieci komputerowych[236]. Tego typu tezy potwierdzały również wcześniejsze wypowiedzi przedstawicieli reżimu KRLD z czerwca 2009, w których zapowiadali pełną gotowość do prowadzenia „wojny *hi-tech*"[237]. Z drugiej jednak strony pojawiły się głosy, które wyrażały sceptycyzm w tym względzie. Na brak jednoznacznych dowodów wskazywali m.in. Jose Nazario oraz Joe Stewart[238]. Wątpliwości te w październiku 2009 roku starał się rozwiać wywiad południowokoreański, który po kilkumiesięcznych badaniach uznał, iż najprawdopodobniej bezpośrednim sprawcą cyberataków było Ministerstwo Poczty i Telekomunikacji KRLD[239]. Ciekawy argument, który potwierdzał tę interpretację zawarto ponadto w raporcie korporacji McAfee z 2011 roku. Stwierdzono w nim, iż wspomniana wiadomość (*Memory of Independence*) zawierała koreański zestaw znaków (*Ten Days of Rain*, 2011: 11).

Warto zauważyć, iż omówione cyberataki wpisywały się w szerszy kontekst relacji międzykoreańskich, a także stosunków KRLD z USA. Poza wspomnianymi już zapowiedziami o gotowości do prowadzenia zaawansowanej tech-

---

[235] J. Markoff, C. Sang-Hun: *Cyberattacks*…, op.cit.

[236] M. Weaver: *Cyber attackers target South Korea and US*…, op.cit.

[237] *North Korea launched cyber attacks, says south*. „The Guardian" 11.07.2009: www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks; dostęp: 3.02.2014.

[238] M. Williams: *Analysis: Was North Korea behind the DDoS attack*? „Computer World" 10.07.2009: www.computerworld.com/s/article/9135406/Analysis_Was_North_Korea_behind_the_DDOS_attack; dostęp: 3.02.2014.

[239] *N. Korean ministry behind July cyber attacks: spy chief*. Yonhap News Agency, 30.10.2009: http://english.yonhapnews.co.kr/northkorea/2009/10/30/0401000000AEN20091030002200315.HTML; dostęp: 3.02.2014.

nologicznie wojny DDoS z lipca 2009 roku współgrał z innymi agresywnymi metodami wywierania nacisku przez Phenian na otoczenie międzynarodowe. Należy pamiętać, iż w połowie roku doszło do całej serii poważnych prowokacji. W maju Korea Północna przeprowadziła drugi próbny wybuch atomowy, w wyniku czego nałożono na nią kolejne sankcje, natomiast na początku lipca reżim rozpoczął testy rakiet balistycznych krótkiego zasięgu typu Rodong, które zostały skierowane na Morze Japońskie. 2 lipca wystrzelono cztery rakiety, kolejnych siedem wzbiło się w powietrzne właśnie w amerykański Dzień Niepodległości — 4 lipca. Wywołało to ostre reakcje m.in. ze strony Korei Południowej, Japonii oraz USA[240]. Doszło do nich w tym samym momencie, w którym rozpoczęła się kampania cyberataków wymierzonych w Waszyngton i Seul. Trudno uwierzyć, aby taka zbieżność była zupełnie przypadkowa. Pionierska dla KRLD akcja w sieci mogła być kolejną próbą oprotestowania decyzji podjętej przez Radę Bezpieczeństwa ONZ 12 czerwca 2009 roku, nakładającej na reżim kolejne sankcje. Obejmowały one m.in. zaostrzenie zakazu handlu bronią, a także niszczenie objętych embargiem towarów zmierzających do Korei Północnej (*Resolution 1874*, 2009). Na tym tle kampania DDoS logicznie wpisywała się więc w prowadzoną również tradycyjnymi środkami serię prowokacji przeciwko USA oraz ich sojusznikom w regionie.

Taką wykładnię potwierdzały kolejne incydenty, które miały miejsce dokładnie 20 miesięcy po wydarzeniach z 2009 roku. 4 marca 2011 roku doszło do kolejnej fali cyberataków typu DDoS wymierzonych w koreańskie oraz amerykańskie strony internetowe. Tym razem główny nacisk został położony na Koreę Południową, w której zablokowano około 40 witryn, zarówno z sektora publicznego, jak i prywatnego. Należy tu wymienić portale należące m.in. do instytucji państwowych (www.assembly.go.kr, www.korea.go.kr, www.customs.go.kr, www.kcc.go.kr, www.nis.go.kr), służb mundurowych oraz wojska (www.police.go.kr, www.navy.mil.kr, www.airfor.mil.kr, www.mnd.mil.kr), serwisów aukcyjnych (www.auction.co.kr), korporacji i przedsiębiorstw (www.daishin.co.kr) oraz banków (www.hanabank.com, www.wooribank.com, www.shinhan.com). Jeśli chodzi natomiast o Amerykanów, to zablokowano jedynie stronę sił USA stacjonujących w Korei Południowej: www.usfk.mil (*Ten Days of Rain*, 2011: 14). Jak zauważyli eksperci koreańskiej korporacji Ahnlab, tym razem w ataku komputerowym wzięło udział jeszcze mniej komputerów — sieć *botnet* złożona była jedynie z ok. 11 000 jednostek[241]. Niemniej jego efekty okazały się nieco

[240] D. Kim: *Fact Sheet: North Korea's Nuclear and Ballistic Missile Programs*. The Center for Arms Control and Non-Proliferation, July 2013: http://armscontrolcenter.org/issues/northkorea/articles/fact_sheet_north_korea_nuclear_and_missile_programs; dostęp: 3.02.2014; *North Korea missile tests defy UN*. BBC News, 04.07.2009: http://news.bbc.co.uk/2/hi/asia-pacific/8134115.stm; dostęp: 3.02.2014.

[241] *South Korea hit by cyber attacks*. BBC News, 04.03.2011: www.bbc.co.uk/news/technology-12646052; dostęp: 3.02.2014.

poważniejsze niż ostatnio, ponieważ do przygotowania i przeprowadzenia kampanii wykorzystano dwa różne programy: trojan *Koredos* i *backdoor* trojan *Prioxer*. Drugi typ był bardziej zaawansowany pod względem zastosowanego kodu, a przez to został wykryty nieco później[242].

Casus ten szybko zainteresował międzynarodowe środowisko naukowe, które podjęło szereg przedsięwzięć badawczych mających za zadanie wyjaśnić jego specyfikę oraz zidentyfikować sprawców. Można tutaj przywołać m.in. raport McAfee Labs, który wskazał na kilka ważnych szczegółów. Przede wszystkim zauważono, iż sieć *botnet* miała ściśle określony czas działania, zaplanowany jedynie na 10 dni, choć operatorzy mogli go przedłużyć w razie potrzeby. Po jego upływie programy kontrolujące poszczególne komputery *zombie* miały się samoistnie usunąć za pomocą tzw. *MBR flash*. Po drugie pierwotne infekcje komputerów złośliwym oprogramowaniem nastąpiły prawdopodobnie przy użyciu południowokoreańskiej witryny internetowej umożliwiającej wymianę plików między użytkownikami. Po trzecie uwagę ekspertów zwróciła struktura serwerów dowodzenia i kontroli sieci *botnet*: okazało się, iż miała ona charakter wielowarstwowy i wyjątkowo skomplikowany, co miało zapobiec szybkiemu przejęciu kontroli nad nią, a tym samym zablokowaniu ataków DDoS. Warto dodać, iż serwery te ulokowane były m.in. w Polsce, Meksyku, Australii, Hong Kongu, Tajlandii, Południowej Afryce, Indiach, Rosji, na Tajwanie oraz w Stanach Zjednoczonych. Po czwarte zastosowano zaawansowane techniki szyfrowania danych, co również miało opóźnić zdobycie kontroli nad *botnetem* przez służby amerykańskie i południowokoreańskie (użyto algorytmów RC4, AES, RSA, MD5). Po piąte wykorzystano różnorodne wektory ataku typu DDOS: ICMP, UDP oraz HTTP. Po szóste w raporcie zwrócono uwagę na podobieństwo do incydentów z 2009 roku, sugerując odpowiedzialność tych samych sprawców. Odnotowano jednak i różnice, do których zaliczono wyższy stopień zaawansowania technicznego oraz odmienne cele. Tym razem witryny amerykańskie stanowiły marginalny obiekt zainteresowania. O wiele większy nacisk położono natomiast na zablokowanie portali armii południowokoreańskiej. Na tej podstawie w raporcie McAfee zasugerowano, iż za cyberatakami z marca 2011 roku stały służby reżimu Kimów, choć nie udało się tego ustalić z całą pewnością (*Ten Days of Rain*, 2011: 1—12).

Już w miesiąc później, w kwietniu 2011 roku, doszło do kolejnego incydentu teleinformatycznego. Tym razem był on zdecydowanie groźniejszy, gdyż celem sprawców stał się jeden z największych południowokoreańskich banków — Nonghyup. W wyniku zainfekowania jego wewnętrznej sieci złośliwym oprogramowaniem na tydzień zablokowano ok. 30 milionom klientów możliwość

[242] *Are the 2011 and 2013 South Korean Cyberattacks Related?* „Symantec Security Response" 29.03.2013: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related; dostęp: 3.02.2014.

korzystania z bankomatów[243]. Było to więc *de facto* pierwsze udane uderzenie wymierzone w południowokoreański sektor finansowy, będący zarazem częścią infrastruktury krytycznej państwa. Po przeprowadzeniu dochodzenia przez służby specjalne okazało się, że przygotowania do cyberataku były stosunkowo długie i staranne, sieć bankowa została bowiem zarażona za pomocą zawierającego złośliwe oprogramowanie komputera przenośnego (notebook) należącego do pracownika IBM, który współpracował od pewnego czasu z Nonghyup. Notebook został zainfekowany już we wrześniu 2010 roku, dzięki czemu uzyskano zdalny dostęp do bankowego intranetu, wyprowadzając stamtąd wrażliwe dane oraz usuwając wybrane pliki. Kulminacja ataku nastąpiła jednak dopiero 12 kwietnia, kiedy za jego pomocą doprowadzono do zablokowania 273 z 587 serwerów bankowych[244]. Był to więc najpoważniejszy dotychczas atak komputerowy przeciwko Korei Południowej. Jej prokuratura po miesiącu prac jednoznacznie obciążyła odpowiedzialnością za incydent KRLD. Oceniając to wydarzenie jako akt cyberterroryzmu, stwierdzono przy tym, iż adres IP serwera dowodzenia i kontroli był taki sam jak w przypadku cyberataku z marca[245].

Warto zauważyć, iż oba przypadki, bez względu na brak niepodważalnych dowodów winy, wpisały się ponownie w tradycyjną kampanię prowokacji ze strony KRLD wobec Korei Południowej. Należy bowiem pamiętać, iż w listopadzie 2010 roku doszło do poważnego ostrzału artyleryjskiego południowokoreańskiej wyspy Yeonpyeong na Morzu Żółtym, co doprowadziło do wymiany ognia po obu stronach granicy[246] i pogorszenia i tak bardzo napiętych relacji dwustronnych. Ponadto regularnie dochodziło do aktów zakłócania systemu GPS przez jednostki wojskowe Korei Północnej, co skutkowało znacznymi utrudnieniami dla południowokoreańskich systemów transportowych i komunikacyjnych. Świadczyło to zarazem o rosnących zdolnościach reżimu w zakresie walki elektronicznej[247]. W czerwcu 2011 roku przeprowadzono natomiast pierwszy od kilkunastu miesięcy test rakiety balistycznej krótkiego zasięgu KN-06. Później ruch ten powtórzono w grudniu. Warto dodać, iż w pierwszej połowie roku reżim zagroził również zerwaniem wszelkich związków z Południem oraz użyciem sił zbrojnych[248]. Cyberatak mógł więc być kolejnym z całej gamy instrumentów

[243] M. Clayton: *In cyberarms race*…, op.cit.

[244] K. Rahn: *NK launched cyber attack on Nonghyup*. „The Korea Times" 03.05.2011: www.koreatimes.co.kr/www/news/nation/2011/05/117_86369.html; dostęp: 4.02.2014.

[245] *North Korea 'behind South Korean bank cyber hack'*. BBC News, 03.05.2011: www.bbc.co.uk/news/world-asia-pacific-13263888; dostęp: 4.02.2014.

[246] H.J. Kim, K.T. Kim: *Korea Attack: Yeonpyeong Island Shelled By North Korea*. „Huffington Post", 23.11.2010: www.huffingtonpost.com/2010/11/23/korea-attack-yeonpyeong-island_n_787294.html#s189509; dostęp: 4.02.2014.

[247] *North Korea's GPS Jamming Prompts South Korea to Endorse Nationwide eLoran System*. „Inside GNSS" 24.04.2013: www.insidegnss.com/node/3532; dostęp: 5.02.2014.

[248] P. Hancocks: *North Korea reportedly test-fires missiles*. CNN, 08.06.2011: http://edition.cnn.com/2011/WORLD/asiapcf/06/07/north.korea.missiles; dostęp: 4.02.2014; *North Korea Test*

nacisku na Seul i Waszyngton. Tym razem celem było wymuszenie wznowienia rozmów wielostronnych po prawie dwuletniej przerwie. Do ponownego spotkania między przedstawicielami reżimu oraz Waszyngtonu doszło w lipcu 2011 roku[249].

Najpoważniejsza seria incydentów teleinformatycznych nastąpiła w 2013 roku. Pierwsze miały miejsce już 20 marca. Tym razem nie odwołano się do sztampowego ataku typu DDoS, lecz bardziej wysublimowanych technik związanych z modyfikowaniem zawartości twardych dysków[250]. Złośliwy program określony mianem *DarkSeoul* o 2.00 w nocy czasu lokalnego zaatakował komputery należące do południowokoreańskich banków (Nonghyup, Jeju, Shinhan, Woori, Nonghyup Insurance) oraz mediów (KBS, MBC oraz YTN). W ciągu kilku minut udało mu się dokonać sabotażu ok. 32 000 jednostek poprzez zepsucie ich głównego rekordu startowego (MBR). W części przypadków miało dojść również do usunięcia wszystkich danych z HDD. Doprowadziło to w konsekwencji do zablokowania niektórych usług sektora finansowego, w szczególności związanych z korzystaniem z bankomatów[251]. *Malware* posiadał również komponent, którego celem było zarażanie nie tylko systemów operacyjnych Windows, lecz również Linux[252]. Ponadto automatycznie starał się wyłączyć dwa popularne w Korei Południowej programy antywirusowe: *Hauri AV* oraz *Ahnlab*[253]. Jak ocenił amerykański zespół US-CERT, program *DarkSeoul* charakteryzował się co prawda stosunkowo prostymi rozwiązaniami technicznymi, te jednak cechowały się wysoką skutecznością. Zdaniem ekspertów został on napisany specjalnie w celu zainfekowania komputerów południowokoreańskich (*South Korean Malware Attacks*, 2013: 1).

Fires 2 Short-Range Missiles From Eastern Coast. Fox News, 19.12.2011: www.foxnews.com/world/2011/12/19/south-korean-news-agency-reports-north-korea-conducts-missile-test-hours-after; dostęp: 4.02.2014.

[249] P. Crail: *U.S., North Korea Hold Bilateral Talks, Arms Control Association*. September 2011: www.armscontrol.org/2011_09/U.S._North_Korea_Hold_Bilateral_Talks; dostęp: 4.02.2014.

[250] *Are the 2011 and 2013 South Korean Cyberattacks Related?* „Symantec Security Response" 29.03.2013: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related; dostęp: 3.02.2014

[251] D. Goodin: *Hard drive-wiping malware that hit South Korea tied to military espionage*. Ars Technica, 08.07.2013: http://arstechnica.com/security/2013/07/hard-drive-wiping-malware-that-hit-s-korea-tied-to-military-espionage, dostep: 4.02.2014; K. Westin: *South Korean Attack & Malware Analysis*. The State of Security, 22.03.2013: www.tripwire.com/state-of-security/security-data-protection/south-korean-attack-malware-analysis; dostęp: 5.02.2014; *South Korea blames North for bank and TV cyber-attacks*. BBC News, 10.04.2013: www.bbc.co.uk/news/technology-22092051; dostęp: 5.02.2014.

[252] K. Zetter: *Logic Bomb Set Off South Korea Cyberattack*. „Wired" 21.03.2013: www.wired.com/threatlevel/2013/03/logic-bomb-south-korea-attack; dostęp: 5.02.2014.

[253] *DarkSeoul Malware attacks major banks of South Korea*. Network Security Blog: www.networksecurity.com/darkseoul-malware-attacks-major-banks-of-south-korea; dostęp: 5.02.2014.

Masowy atak komputerowy spotkał się oczywiście z reakcją władz w Seulu, które podniosły stan Internet Security Response do poziomu „alarm". Prezydent kraju zwrócił się do podległych mu służb o wyjaśnienie, kto jest bezpośrednio odpowiedzialny za atak[254]. Początkowo podejrzenie padło na dwie grupy hakerskie. Jedną była New Romanic Cyber Army Team, która w tym samym czasie włamała się na stronę Nocut News Korea, gdzie zamieściła informację, w której przyznano się do zorganizowania tej akcji. O odpowiedzialności tej grupy świadczyły także elementy kodu *DarkSeoul*, które nawiązywały do rzymskiej armii (słowa *hastati* czy *principes*); jego ścieżka dostępu zawierała też nawiązania do starożytnej Troi. Drugą oskarżaną grupą była The WhoIS Hacking Team, która 20 marca 2013 roku zamieniła zawartość witryny dostawcy usług internetowych LG+U, ta jednak nie przyznała się do wzięcia udziału we włamaniu. W obu przypadkach pojawiały się pewne wskazówki świadczące o ich możliwej odpowiedzialności, nie były one jednak na tyle mocne, aby jednoznacznie o tym przesądzać. Warto dodać, iż trojan, który wykorzystano do akcji, został skompilowany dopiero 26 stycznia 2013 roku. Później, kilka tygodni przed właściwym włamaniem, zarażono sieci bankowe za pomocą ataku typu *spear-phishing*. Wszystkie te zabiegi miały na celu zebranie niezbędnych danych do tego, aby właściwe uderzenie okazało się jak najbardziej bolesne (Sherstobitoff, Liba, Walter, s. 3—6).

Na tym tle można odwołać się do raportu korporacji McAfee, według którego incydent ten był tylko jednym z elementów wieloletniej operacji cyberszpiegowskiej wobec Korei Południowej. Jak stwierdzili jego autorzy, kampania ta, określona mianem *Troy*, była prowadzona już od 2009 roku, kiedy stworzono zręby złośliwego kodu przeznaczonego do zbierania poufnych danych. Ich zdaniem aż do 2013 roku prowadzono niewykryte cyberataki o charakterze wywiadowczym, których celem było zdobycie informacji przydatnych do organizowania kolejnych włamań. W 2010 roku opracowano pierwszą wersję oprogramowania *Troy* (NSTAR) bazującą na rozwiązaniach wojskowych. W 2011 roku powstał trojan *HTTP Troy*, który instalował na komputerze zdjęcia tonącego południowokoreańskiego okrętu wojennego *Ch'onan* zniszczonego, jak wspomniano, przez KRLD w 2010 roku. W 2012 roku sprawcy wykorzystywali natomiast kolejne typy złośliwych programów: *Dr0pper* oraz *Tong*. W 2013 roku użyto złośliwego programu o nazwie *TDrop* oraz *Concealment Troy*. Zdaniem McAfee Labs wszystkie miały być związane z incydentem *DarkSeoul.* Głównym celem działania sprawców według dokumentu było zbieranie informacji o sieciach wojskowych Korei Południowej. Zastosowane złośliwe oprogramowanie miało także możliwość usunięcia wszystkich danych z zainfekowanych komputerów. Rea-

[254] *Wiper Malware Analysis Attacking Korean Financial Sector.* Dell SecureWorks, 21.03.2013: www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector; dostęp: 5.02.2014.

sumując, w raporcie stwierdzono, że wszystkie poważne incydenty teleinformatyczne, które miały miejsce w Korei Południowej w latach 2009—2013, były wynikiem działania tajnego programu szpiegowskiego wymierzonego w jej sieci rządowe i wojskowe. Nie przesądzono jednak ostatecznie, kto był ich organizatorem (Ibidem, s. 4—28).

Również inne ośrodki eksperckie były bardzo ostrożne w ferowaniu wyroków w tej sprawie. Dell SecureWorks wśród możliwych sprawców ataku komputerowego wymienił nie tylko Koreę Północną, lecz także Chiny oraz grupę WhoIS. Zaznaczono przy tym, że nie odnaleziono wystarczających dowodów, które mogłyby potwierdzić którąś z tych tez[255]. Z kolei analitycy Avast stwierdzili, że akcja została przeprowadzona z terytorium ChRL, o czym miało świadczyć m.in. występowanie w kodzie trojana chińskich słów (np. *tongji*, *tong*, *pao*)[256]. Wątpliwości takich nie miały jednak południowokoreańskie służby, które po przeprowadzonym dochodzeniu po raz kolejny winą za incydenty obarczyły reżim Kimów. Zdaniem Seulu część złośliwego oprogramowania z 20 marca była bardzo podobna do rozwiązań znanych już z poprzednich lat. Jak ujawniono, aż 30 z 76 programów wykorzystanych w tym ataku było już wcześniej użytych przeciwko Korei Południowej. Ponadto z 49 zidentyfikowanych adresów IP komputerów, z których korzystali sprawcy, 22 wykryto w przeszłości, dlatego władze południowokoreańskie wskazały na odpowiedzialność Głównego Biura Wywiadowczego (RGB) KRLD[257]. Interpretację tę potwierdzały zresztą doniesienia medialne, według których w prywatnych rozmowach eksperci McAfee również mieli wskazywać jednoznacznie na sprawstwo Phenianu[258].

Kolejna fala cyberataków wymierzonych w Koreę Południową rozpoczęła się 25 czerwca 2013 roku, w 63. rocznicę rozpoczęcia wojny koreańskiej. Trwała ona aż do 1 lipca. Za pomocą metody DDoS sparaliżowano wówczas rekordową liczbę 69 witryn internetowych należących do instytucji państwowych, mediów oraz największych przedsiębiorstw. Wśród nich można wymienić strony m.in. prezydenta, premiera, ministerstw, partii politycznych, 11 ośrodków medialnych oraz 4 agencji rządowych. Zawartość niektórych zaatakowanych portali została zamieniona (*web defacement*), zamieszczono na nich materiały wskazujące wyraźnie na bezpośredni udział służb Korei Północnej, w tym np. hasła typu *Wielki Przywódca Kim Dzong Un*. Sprawcy zastosowali w sumie 82 skrypty

---

[255] *Wiper Malware Analysis Attacking Korean Financial Sector*. Dell SecureWorks, 21.03.2013: www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector; dostęp: 5.02.2014.

[256] *Seoul cautious in blaming North Korea for massive cyberattack*. „Infosecurity Magazine" 20.03.2013: www.infosecurity-magazine.com/view/31372/seoul-cautious-in-blaming-north-korea-for-massive-cyberattack-; dostęp: 5.02.2014.

[257] *South Korea blames North for bank and TV cyber-attacks*. BBC News, 10.04.2013: www.bbc.co.uk/news/technology-22092051; dostęp: 5.02.2014.

[258] M. Clayton: *In cyberarms race*…, op.cit.

komputerowe, które częściowo były już używane w poprzednich akcjach tego typu[259]. Jak zauważyli eksperci, masowy charakter oraz skuteczność tych cyberataków świadczyły o tym, iż musiały być one przygotowywane od dłuższego czasu. Ponadto zastosowano tutaj ciekawy sposób infekowania komputerów: wykorzystano do tego popularny serwis wymiany i przechowywania plików w południowokoreańskim Internecie — SimDisk. W związku z tym specjaliści z Trend Micro wysoko ocenili poziom zaawansowania technicznego całej operacji[260]. Warto dodać, iż tym razem równolegle doszło do ataków na strony internetowe Korei Północnej. Jak się jednak szybko okazało, za tymi incydentami stała grupa haktywistyczna Anonymous. Pojawiały się wówczas pewne wątpliwości, czy nie była ona również odpowiedzialna za wydarzenia w Korei Południowej, szybko jednak odrzucono te przypuszczenia. Po raz kolejny natomiast Seul oskarżył o organizację cyberataków reżim w Phenianie. 26 lipca 2013 roku wypowiedział się na ten temat jeden z przedstawicieli rządu Park Jae Moon[261].

We wrześniu 2013 roku wybuchła w Korei Południowej kolejna afera cyberszpiegowska. 11 września ekspert Kaspersky Lab Dmitry Tarakanov opublikował raport na temat działań wywiadowczych w sieci, wymierzonych głównie w tamtejsze ośrodki badawcze, uniwersytety, przedsiębiorstwa oraz instytucje rządowe. Do spenetrowanych instytucji zaliczył on m.in.:

- Sejong Institute prowadzący badania nad strategią bezpieczeństwa narodowego, strategią zjednoczenia Półwyspu Koreańskiego, międzynarodowymi stosunkami gospodarczymi oraz wybranymi wyzwaniami regionalnymi;
- Korea Institute for Defense Analysis (KIDA) będący instytucją badawczą zajmującą się głównie tematyką bezpieczeństwa i obrony, w tym planowaniem

[259] M.J. Schwartz: *Anonymous Not Behind Attacks South Korea Says*. „Information Week" 16.07.2013: www.informationweek.com/attacks/anonymous-not-behind-attacks-southkorea-says/d/d-id/1110771?; dostęp: 5.02.2014; *North and South Korea Hit By Cyber Attacks*. Sky News, 25.07.2013: http://news.sky.com/story/1107894/north-and-south-korea-hit-by-cyber-attacks; dostęp: 5.02.2014; C. Sang-Hun: *South Korea Blames North for June Cyberattacks*. „The New York Times" 16.07.2013: www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0; dostęp: 5.02.2014; *North and South Korea websites shut amid hacking alert*. „The Guardian" 25.07.2013: www.theguardian.com/world/2013/jun/25/north-korea-south-websites-hacking-cyber-attack; dostęp: 5.02.2014; E. Shim, Y. Lee: *South Korea issues cyberattack alert after it says many sites are hacked*. World News, 25.06.2013: http://worldnews.nbcnews.com/_news/2013/06/25/19124890-south-korea-issues-cyberattack-alert-after-it-says-many-sites-are-hacked?lite; dostęp: 4.02.2014.

[260] *Trend Micro Investigates June 25 Cyber Attacks in South Korea*. Trend Micro: http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Trend+Micro+Investigates+June+25+Cyber+Attacks+in+South+Korea&tab=malware; dostęp: 5.02.2014.

[261] *South Korea blames North Korea for cyberattack on media, government sites*. Fox News, 16.07.2013: www.foxnews.com/world/2013/07/16/south-korea-blames-north-korea-for-cyberattack-on-media-government-sites; dostęp: 4.02.2014; M.J. Schwartz: *Anonymous Not Behind Attacks South Korea Says*. „Information Week" 16.07.2013: www.informationweek.com/attacks/anonymous-not-behind-attacks-south-korea-says/d/d-id/1110771?; dostęp: 5.02.2014.

militarnym, rozwojem zasobów ludzkich, zarządzaniem środkami, systemami uzbrojenia, systemami informacyjnymi oraz modelowaniem i symulacjami;
- Ministerstwo Zjednoczenia (Ministry of Unification) odpowiedzialne za wszystkie działania zmierzające do reunifikacji obu państw koreańskich, w tym np. dialog międzykoreański;
- Hyundai Merchant Marine będące przedsiębiorstwem zajmującym się logistyką morską.

Jak stwierdzono w dokumencie, eksperci Kaspersky Lab wykryli operacje cyberszpiegowskie wymierzone w 11 podmiotów południowokoreańskich oraz 2 chińskie. Wszystkie były w mniejszym lub większym stopniu związane z obronnością, bezpieczeństwem, stosunkami międzynarodowymi bądź sprawami międzykoreańskimi. Zauważono również, że cyberataki o podłożu wywiadowczym miały bardzo ograniczony charakter oraz były precyzyjnie wymierzone w najbardziej wrażliwe punkty. Ponadto zastosowane przez sprawców złośliwe oprogramowanie dawało duże możliwości zbierania danych z zarażonych komputerów, w tym m.in. pozyskiwania nazw użytkownika i haseł, zdalnej kontroli dostępu, a także kopiowania zawartości twardych dysków. Całą operację, podobnie jak użytego trojana, określono mianem *Kimsuky*. Na tej podstawie analitycy korporacji wskazali na prawdopodobną odpowiedzialność służb KRLD, o czym miały świadczyć koreańskie znaki i słowa znalezione w kodzie programu[262].

Na tym tle widać więc wyraźnie, iż w 2013 roku nastąpiła kulminacja incydentów teleinformatycznych wymierzonych w Koreę Południową. Jak zauważył Tobias Feakin (2013: 84—85), nie przyniosły one co prawda kinetycznych zniszczeń, doprowadziły jednak do poważnych utrudnień korzystania z określonych usług sieciowych, a także do strat zarówno w wymiarze finansowym, jak i prestiżowym. Według niego regularnie powtarzające się cyberataki stanowiły czynnik destabilizujący sytuację gospodarczą w kraju, potencjalni inwestorzy mogli bowiem zostać zniechęceni do poszerzania swojej aktywności na Półwyspie. We wszystkich przypadkach zdecydowana większość ekspertów, a także służb południowokoreańskich, wskazywała na odpowiedzialność reżimu Kim Dzong Una. Taką interpretację potwierdzały zresztą kolejne wydarzenia w stosunkach międzykoreańskich oraz na linii Phenian — Waszyngton. Podobnie jak w poprzednich latach widoczna była daleko idąca korelacja między cyberatakami a innymi prowokacjami ze strony Północy. Należy pamiętać, że 12 grudnia 2012 roku Korea Północna wystrzeliła w kosmos satelitę obserwacyjnego Kwangmyongsong-3 Unit-2, co zbiegło się w czasie z obchodami pierwszej rocznicy śmierci Kim

[262] D. Tarakanov: *The „Kimsuky" Operation: A North Korean APT?* SecureList, 11.09.2013: www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT; dostęp: 5.02.2014; D. Tarakanov: *Kimsuky APT: Operation's possible North Korean links uncovered*. SecureList, 11.09.2013: www.securelist.com/en/blog/208214062/Kimsuky_APT_Operations_possible_North_Korean_links_uncovered; dostęp: 5.02.2014.

Dzong Ila oraz wyborami prezydenckimi w tym kraju[263]. Wydarzenie to wywołało ostrą reakcję całej społeczności międzynarodowej. Jej wyrazem była rezolucja Rady Bezpieczeństwa ONZ nr 2087 uchwalona 22 stycznia 2013 roku, w której potępiono Phenian za złamanie zakazu testów broni balistycznej oraz wzmocniono sankcje (*Security Council*, 2013). Doprowadziło to do znacznej eskalacji napięcia w całej Azji Wschodniej. W dwa dni później KRLD zapowiedziała przeprowadzenie kolejnych testów broni atomowej, co nastąpiło ostatecznie w pierwszej połowie lutego i zostało ostro skrytykowane przez społeczność międzynarodową oraz doprowadziło do nałożenia kolejnych sankcji[264]. W odpowiedzi na to, a także na wspólne manewry koreańsko-amerykańskie, reżim Kim Dzong Una w marcu wycofał się z układu o zawieszeniu broni z 1953 roku oraz zagroził „bezwzględną" odpowiedzią militarną. 30 marca stwierdził, iż znajduje się w stanie wojny z Koreą Południową. W kwietniu natomiast Phenian zapowiedział wznowienie prac w ośrodku atomowym w Yongbyon oraz wycofanie pracowników z parku przemysłowego Kaesong, co w konsekwencji doprowadziło do szeregu nerwowych ruchów wojsk, zarówno ze strony Korei Północnej, Południowej, jak i Stanów Zjednoczonych, do których można zaliczyć m.in. przelot dwóch bombowców B-2 Spirit nad Półwyspem Koreańskim pod koniec marca czy test czterech rakiet balistycznych krótkiego zasięgu przeprowadzony przez Phenian w maju[265]. W końcu Korea Północna została jednak zmuszona do poszukiwania kompromisu. Wyrazem tego była czerwcowa sugestia o gotowości do wznowienia wielostronnych rozmów w sprawie jej programu atomowego[266].

Eskalacja incydentów teleinformatycznych z 2013 roku zbiegła się więc wyraźnie w czasie z ponownym wzrostem napięcia w stosunkach na linii Phe-

[263] *North Korea profile*. BBC News, 17.12.2013: www.bbc.co.uk/news/world-asia-pacific-15278612; dostęp: 5.02.2014; M. Park, P. Hancocks, K.J. Kwon, *Park Geun-hye claims South Korea presidential victory*. CNN, 19.12.2012: http://edition.cnn.com/2012/12/18/world/asia/south-korea-presidential-election; dostęp: 5.02.2014.

[264] *North Korea nuclear tests*. BBC News, 12.02.2013: www.bbc.co.uk/news/world-asia-17823706; dostęp: 5.02.2014; R. Gladstone: *New Sanctions on North Korea Pass in Unified U.N. Vote*. „The New York Times" 07.03.2013: www.nytimes.com/2013/03/08/world/asia/north-korea-warns-of-pre-emptive-nuclear-attack.html?pagewanted=all; dostęp: 5.02.2014.

[265] W. Strobel: *U.S. B-2 bombers sent to Korea on rare mission: diplomacy not destruction*. Reuters, 30.03.2013: www.reuters.com/article/2013/03/30/us-korea-north-usa-b-idUSBRE92S0IE20130330; dostęp: 5.02.2014; J. Kim: *North Korea says enters 'state of war' against South*. Reuters, 30.03.2013: www.reuters.com/article/2013/03/30/us-korea-north-war-idUSBRE92T00020130330; dostęp: 5.02.2014; L. Chang-Won: *North Korea confirms end of war armistice*. AFP, 13.03.2013: www.google.com/hostednews/afp/article/ALeqM5ihNf_P_yjcx87RS5q6V7XIM9xduA?docId=CNG.9853b860fe89106d015080a384fbfdf4.491; dostęp: 5.02.2014; *North Korea profile*. BBC News, 17.12.2013: www.bbc.co.uk/news/world-asia-pacific-15278612; dostęp: 5.02.2014; *North Korea profile*. BBC News, 17.12.2013: www.bbc.co.uk/news/world-asia-pacific-15278612; dostęp: 5.02.2014.

[266] *North Korea, China want to resume nuclear talks*. CCN, 19.06.2013: http://edition.cnn.com/2013/06/19/world/asia/nk-china-nuclear-dialogue/index.html; dostęp: 5.02.2014.

nian — Seul — Waszyngton. Ataki z 20 marca wpisały się widocznie w apogeum kryzysu na Półwyspie, kiedy Kim Dzong Un wykorzystywał wszystkie dostępne mu środki, aby wymusić korzystne dla siebie reakcje ze strony innych państw w regionie. W przypadku wydarzeń z czerwca mogły one służyć jako dodatkowy sposób nacisku na Koreę Południową oraz USA, aby wznowić rozmowy sześciostronne.

Reasumując, należy podkreślić, iż relacje między Koreą Północną a Południową są od zarania bardzo trudne i stwarzają poważne zagrożenie dla bezpieczeństwa Azji Wschodniej. Mimo wielu prób zbliżenia reżim w Phenianie był w niewielkim stopniu zainteresowany rzeczywistą rekoncyliacją z rządem w Seulu i stosował wobec niego, a także innych państw aktywnych na Półwyspie, strategię charakteryzującą się z jednej strony pozornym zbliżeniem, z drugiej regularnymi prowokacjami. Znaczna część z nich miała charakter militarny, co wielokrotnie stawiało oba państwa na granicy kolejnej wojny. Wraz z postępem rewolucji teleinformatycznej oba kraje w odmienny sposób podeszły do związanych z nią korzyści. Korea Południowa stała się jednym z najbardziej zaawansowanych technologicznie krajów świata, jednak niewielką wagę przykładano do wykorzystania cyberprzestrzeni jako nowego środka oddziaływania na środowisko międzynarodowe. W przypadku stosunków z reżimem Kimów było to tym bardziej pozbawione sensu, iż był on niemal zupełnie odcięty od światowej infrastruktury internetowej. Mimo ogromnego zapóźnienia w tej dziedzinie Phenian bardzo szybko dostrzegł przydatność cyberataków do osiągania własnych interesów, przede wszystkim w stosunkach z Seulem, a w mniejszym stopniu również z innymi państwami, przez lata rozwijał zatem swoje zdolności w tej dziedzinie, po czym w 2009 roku podjął pierwsze próby ich praktycznego zastosowania. Miały one w założeniu stanowić jeden z wielu środków wywierania nacisków na przeciwników reżimu, tak aby wymusić korzystne dla siebie rozwiązania i decyzje. Tym samym z perspektywy teorii polityki zagranicznej wpisywało się to we wzmacnianie pozycji oraz prestiżu państwa w stosunkach międzynarodowych i dało początek wieloletniej kampanii regularnych cyberataków wymierzonych w instytucje rządowe, służby, media oraz sektor finansowy Korei Południowej. Początkowo miały one mało zaawansowany charakter, w kolejnych latach zaczęły jednak stanowić coraz poważniejsze zagrożenie dla jej bezpieczeństwa narodowego. Jeśli porównać te incydenty np. do *casusu* Estonii czy Gruzji, widać dobitnie, iż udało się w zdecydowanie większym stopniu naruszyć elementy systemu finansowego państwa, a tym samym wpłynąć na funkcjonowanie infrastruktury krytycznej, dlatego przynajmniej część z nich można sklasyfikować jako akty cyberterroryzmu lub cyberszpiegostwa. Oczywiście nie ma zupełnej pewności co do odpowiedzialności Korei Północnej za te ataki, sprawcy bowiem umiejętnie wykorzystywali jedną z podstawowych cech Internetu, jaką jest łatwa do osiągnięcia anonimowość. Niemniej o winie reżimu świadczyły nie tylko wszystkie przytoczone wyżej informacje, ale i bezpośred-

nie motywy. Żaden inny kraj lub ich grupa nie miałyby interesu w tym, aby przez tak długi czas prowadzić tak intensywną kampanię wymierzoną w te same instytucje południowokoreańskie. Można się więc zgodzić z Tobiasem Feakinem (2013: 87—88), którego zdaniem ostatnie dowody jasno wskazują na fakt, iż Phenian zamierza wykorzystywać zdolności do działań w cyberprzestrzeni równolegle z innymi tradycyjnymi środkami „potrząsania szablą", takimi jak agresywna retoryka czy ograniczone ataki wojskowe. Według niego „zdolność Korei Południowej do odpowiedzi na te incydenty […] będzie jeszcze jednym wyzwaniem do rozważenia dla planistów strategicznych na Półwyspie", czego wynikiem powinna być dojrzała „cyberpolityka", zdolna do powstrzymania radykalnych „cyberprowokacji". Można zatem potwierdzić, iż cyberprzestrzeń stała się na przełomie pierwszej i drugiej dekady XXI wieku kolejnym wymiarem rywalizacji pomiędzy dwoma państwami koreańskimi.

4.8. Cyberwojna w stosunkach amerykańsko-chińskich

Aby zrealizować postawiony we wstępie cel badawczy, należałoby omówić również rolę cyberprzestrzeni w stosunkach amerykańsko-chińskich, jest to bowiem jeden z najbardziej widocznych i zarazem unikalnych przykładów rosnącego znaczenia cyberataków w stosunkach międzynarodowych. Wynika to z trzech czynników: ich liczby, długotrwałości oraz konsekwencji dla różnych płaszczyzn relacji bilateralnych. Warto szerzej scharakteryzować to zagadnienie, rozpoczynając od przedstawienia ich podstawowych uwarunkowań.

Przede wszystkim warto zauważyć, iż stosunki amerykańsko-chińskie mają relatywnie długą tradycję, ponieważ pierwsze kontakty nawiązano już w drugiej połowie XVIII wieku. Mimo dość aktywnego zaangażowania USA w Chinach w XIX wieku stosunki z Pekinem zyskały na znaczeniu dopiero po zakończeniu drugiej wojny światowej. USA sprzymierzone z rządem z Chongqingu negatywnie przyjęły bieg wydarzeń w Państwie Środka, w których wyniku wojnę domową w tym kraju pod koniec lat 40. wygrali komuniści pod wodzą Mao Tse Tunga. Niezgoda na uznanie nowego reżimu doprowadziła do serii poważnych napięć, których apogeum była wojna koreańska w latach 1950—1953. Doszło wówczas do pierwszych walk między USA a Chinami od czasu powstania bokserów na przełomie wieków. Stosunki dwustronne w warunkach zimnowojennych zostały ustabilizowane dopiero pod koniec lat 70. XX wieku, kiedy Waszyngton zapowiedział oficjalne uznanie Chińskiej Republiki Ludowej[267]. Mimo nawią-

[267] *Timeline: U.S. Relations with China*. Council on Foreign Relations: www.cfr.org/china/us-relations-china-1949---present/p17698; dostęp: 12.02.2014; *Chronology of U.S.-China Rela-*

zania kontaktów dyplomatycznych relacje bilateralne pozostały napięte, na co wpływ miała nie tylko kwestia niezależności Tajwanu, ale także autorytarny charakter systemu politycznego ChRL, politycy amerykańscy bowiem wielokrotnie podkreślali potrzebę ochrony praw człowieka w tym kraju, co zaczęło być szczególnie mocno akcentowane w 1989 roku, po wydarzeniach na placu Tiananmen (McFadden, 1989).

W okresie pozimnowojennym polityka amerykańska wobec Chińskiej Republiki Ludowej uległa daleko idącej modyfikacji. Po 1989 roku, jak słusznie stwierdziła Justyna Zając (2011: 61), Stany Zjednoczone stały się niekwestionowanym hegemonem, który posiadał „wszelkie atrybuty do sprawowania światowego przywództwa: potencjał, zgodę innych państw na odgrywanie roli przywódczej, a także wolę pełnienia takiej funkcji. USA dysponowały największym potencjałem militarnym i ekonomicznym oraz jednymi z najskuteczniejszych instrumentów oddziaływania politycznego". Początkowo pełnienie roli przywódczej na świecie wiązało się z realizacją idei „nowego ładu światowego", sformułowanej przez George'a Busha. Później globalne cele polityki amerykańskiej doprecyzowano w okresie prezydentury Billa Clintona. Za główne jej priorytety uznano umacnianie bezpieczeństwa, wspieranie narodowego dobrobytu oraz promocję demokracji (Ibidem, s. 63—64). Założenia te rodziły obiektywne trudności w stosunkach z Chińską Republiką Ludową. Jak zauważył Marcin Kaczmarski (2006: 161), główną przesłanką, która determinowała relacje dwustronne z perspektywy Waszyngtonu, było początkowo zniknięcie wspólnego wroga, jakim był Związek Radziecki. Dynamicznie rozwijająca się ChRL zyskała zatem możliwość zdobycia czołowej pozycji zarówno w Azji Wschodniej, jak i na całym świecie. Na tym tle widoczny stał się konflikt interesów pomiędzy posiadającym dominującą pozycję Waszyngtonem a Pekinem. W latach 90. XX wieku stosunki bilateralne warunkowało wiele kwestii. Wśród nich można wymienić m.in. wzrost znaczenia kwestii humanitarnych i ochrony praw człowieka, wojnę w Zatoce Perskiej w 1991 roku, która ukazała Chińczykom skalę przewagi technologicznej USA nad resztą świata, nawiązanie do tzw. polityki jednych Chin (w Narodowej Strategii Bezpieczeństwa USA z 1996 roku), utrzymanie strategicznego dialogu, a także zwiększenie stabilności w Cieśninie Tajwańskiej (Ibidem, s. 162).

Bez wątpienia w tym czasie za najpoważniejszą sprawę uchodziła kwestia tajwańska. Stosunki na linii Pekin — Tajpej oraz Waszyngton — Tajpej tradycyjnie wywoływały poważne napięcia po obu stronach Pacyfiku. W latach 1995—1996 problem ten doprowadził np. do wyraźnego kryzysu na linii USA — ChRL, ponieważ po testach rakiet balistycznych przeprowadzonych przez Chiny w pobliżu Tajwanu prezydent Clinton zdecydował się w marcu 1996 roku wysłać w okolice wyspy dwie grupy lotniskowców (Kan, Morrison, 2013: 5).

---

tions, 1784—2000. Office of the Historian U.S. Department of State: https://history.state.gov/countries/issues/china-us-relations; dostęp: 12.02.2014.

Do dalszej zmiany w polityce wobec Chińskiej Republiki Ludowej doszło na początku XXI wieku, kiedy urząd prezydenta Stanów Zjednoczonych objął George W. Bush. Dostrzegając sygnały coraz szybszego rozwoju gospodarczego, technologicznego i wojskowego Chin, Waszyngton zdecydował się podjąć pierwsze kroki sygnalizujące zamiar redukcji swoich sił zbrojnych w Europie na rzecz większej obecności w Azji Wschodniej. Przejawem tego miało być zacieśnienie stosunków z Japonią, Koreą Południową i Tajwanem oraz aktywna i twarda polityka wobec Pekinu. Te zamierzenia w dużej mierze zostały jednak przekreślone przez zamachy terrorystyczne na World Trade Center 11 września 2001 roku. Wówczas uwaga amerykańskiej dyplomacji skupiła się głównie na Szerokim Bliskim Wschodzie (Kaczmarski, 2006: 162—163). Niemniej obiektywna rola Chin w polityce zagranicznej USA na początku XXI wieku stale rosła, co wynikało z dwóch przesłanek: determinował to wspomniany już dynamiczny rozwój ChRL na wielu płaszczyznach[268], a ponadto wpływ na to miała coraz większa aktywność Pekinu w różnych częściach świata, co oznaczało powstawanie nowych wyzwań dla dotychczas uprzywilejowanej pozycji Stanów Zjednoczonych. Z jednej strony przejawem tych tendencji była narastająca rywalizacja amerykańsko-chińska w Afryce, w głównej mierze na tle dostępu do złóż surowców energetycznych (zob. Lafargue, 2005: 43—56; Hong, 2007), z drugiej polityka chińska rodziła znaczne trudności dla Waszyngtonu na obszarze Szerokiego Bliskiego Wschodu. Przejawem tego były m.in. sprzeciw Pekinu wobec interwencji amerykańskiej w Iraku (Czornik, 2011: 237) czy rosnąca obecność w Afganistanie (zob. Huasheng, Kuchins, 2012).

Wzmocnienie pozycji ChRL na arenie międzynarodowej było tym bardziej widoczne, że w okresie prezydentury George'a W. Busha stopniowej degradacji ulegała ranga Stanów Zjednoczonych. Jak słusznie stwierdziła Jadwiga Stachura (2007: 147—148), w połowie pierwszej dekady XXI wieku na podkopanie supermocarstwowego statusu USA złożyło się kilka czynników: obniżenie wiarygodności Waszyngtonu, słabość amerykańskiego przywództwa, wzrost potencjałów Chin i Indii, a także skuteczność „rywali oraz okazjonalnych oponentów w posługiwaniu się instrumentami typu *soft balancing*". Szczególną uwagę autorka zwróciła właśnie na Chiny, które jej zdaniem „postrzegane jako supermocarstwo w przyszłości, konsekwentnie dążą do zmniejszenia amerykańskiej przewagi w najważniejszych dziedzinach (gospodarka, nowoczesne technologie, obronność) przy jednoczesnym umacnianiu swej pozycji w regionie oraz zwiększaniu wpływów na innych kontynentach". W tym kontekście nie dziwi więc fakt, iż jednym z podstawowych celów amerykańskiej polityki zagranicznej wobec Azji było powstrzymanie wzrostu chińskiej potęgi oraz wpływów na świecie. W czasie prezydentury George'a W. Busha podejmo-

[268] Przykładowo w latach 1978—2011 średni roczny wzrost gospodarczy Chin oscylował w granicach 10% PKB. Zob. Haltmaier, 2013.

wano więc wielowymiarowe działania w tym kierunku, wśród których można wymienić utrzymanie *status quo* w kwestii Tajwanu, budowę systemu obrony przeciwrakietowej, rozwijanie współpracy wojskowej z Japonią i Koreą Południową, podkreślanie znaczenia przestrzegania praw człowieka, a także wysiłki na rzecz rozwiązania kryzysu na Półwyspie Koreańskim (Kaczmarski, 2006: 163—173).

Do kolejnej zasadniczej zmiany w amerykańskiej strategii wobec Chin doszło w czasie prezydentury Baracka Obamy. Zaraz po objęciu urzędu w 2009 roku podjął on szereg decyzji świadczących o znaczących przewartościowaniach w polityce zagranicznej USA, charakteryzujących się widocznym przeniesieniem punktu ciężkości ze strefy euroatlantyckiej w kierunku Azji Wschodniej. Z jednej strony był to więc powrót do koncepcji, która pojawiła się już u George'a W. Busha, z drugiej ruch ten był naturalną konsekwencją stopniowego zmierzchu hegemonicznego statusu Stanów Zjednoczonych na arenie międzynarodowej, zarówno w płaszczyźnie politycznej, jak i gospodarczej. Symbolicznym przejawem tych procesów był m.in. kryzys finansowy zapoczątkowany w USA w 2008 roku (Grosse, 2013: 193). Należy się więc zgodzić ze słowami Jadwigi Kiwerskiej (2012: 34), która stwierdziła, iż

> u progu drugiej dekady XXI w. Stany Zjednoczone, chcąc nie chcąc, musiały konkurować na geopolitycznym rynku z innymi potęgami […]. I to pomimo tego, że nadal Ameryka jako jedyna dysponowała wszystkimi naraz atrybutami supermocarstwowości: ekonomicznymi, militarnymi, technologicznymi i politycznymi […]. W każdym razie jednym z najważniejszych zjawisk pierwszej dekady XXI w. było pojawienie się nowych potęg, których pozycję w dużym stopniu określał zwiększony potencjał gospodarczy.

W tej trudnej dla Waszyngtonu sytuacji Biały Dom podjął działania, które sygnalizowały spadające zainteresowanie Europą na rzecz Azji. Świadczyło o tym dobitnie oświadczenie Baracka Obamy z maja 2011 roku, w którym zadeklarował, iż XXI wiek będzie dla USA wiekiem Pacyfiku (Matera, 2012: 74). Wystąpienie to zbiegło się w czasie z decyzją o cięciach wydatków na obronę oraz zapowiedzią ograniczenia amerykańskich sił wojskowych na Starym Kontynencie. Miało temu towarzyszyć zwiększanie obecności w strefie Azji i Pacyfiku (np. w północnej Australii) oraz poszerzenie współpracy militarnej z sojusznikami w tym regionie, w tym m.in. z Singapurem oraz Filipinami (Kiwerska, 2012: 52).

Wszystkie wymienione wyżej decyzje, tendencje i działania miały fundamentalny związek z Chińską Republiką Ludową, administracja Obamy doszła bowiem do słusznego wniosku, iż to Pekin wyrasta na główne zagrożenie dla supermocarstwowej pozycji USA na świecie. Jak pisała Aleksandra Jarczewska (2013: 95), najważniejszymi wyzwaniami dla amerykańskich relacji z Chinami były wówczas „zwiększająca się siła oraz aktywność ChRL w regio-

nie […], pogłębiające się współzależności gospodarcze oraz zaostrzający się amerykańsko-chiński konflikt w cyberprzestrzeni". Najbardziej widocznym przejawem tego typu tendencji stały się narastające napięcia wynikające z chińskich roszczeń terytorialnych na Morzu Południowochińskim i Wschodniochińskim. Dotyczyły one m.in. kontrolowanych przez Japonię wysp Senkaku (zob. Dolven, Kan, Manyin, 2013). Nie dziwi więc fakt, iż jednym z fundamentalnych celów polityki zagranicznej prezydenta Baracka Obamy stało się powstrzymanie rosnącej potęgi Chińskiej Republiki Ludowej oraz zapewnienie realizacji amerykańskich interesów narodowych na obszarze Azji Wschodniej i Pacyfiku (Park, 2013: 4).

Podobne, konfrontacyjne nastawienie wobec Stanów Zjednoczonych było widoczne w okresie pozimnowojennym w polityce zagranicznej Chińskiej Republiki Ludowej. Oficjalnie oczywiście miała ona charakter pokojowy i koncyliacyjny. Za Joanną Marszałek-Kawą (2011: 115) można wskazać na kilka jej podstawowych założeń:

- promowanie multipolarnego porządku międzynarodowego,
- stymulowanie i promowanie rozwoju ekonomicznej globalizacji,
- wsparcie koncepcji bezpieczeństwa opartego na konsultacjach w atmosferze wzajemnego zaufania,
- promowanie dyplomacji wielostronnej,
- utrzymywanie długoterminowych relacji z państwami sąsiadującymi,
- wzmacnianie solidarności i współpracy z krajami rozwijającymi się,
- budowa harmonijnego ładu światowego opartego na przyjaznych relacjach między państwami,
- zwalczanie problemów globalnych, takich jak rozprzestrzenianie broni masowego rażenia, walka z terroryzmem oraz kryzysem gospodarczym.

Analitycy Center for Strategic & International Studies powyższe priorytety skonkretyzowali w dwóch celach polityki zagranicznej ChRL dotyczących utrzymania chińskiej niepodległości, suwerenności oraz integralności terytorialnej i wytworzenia korzystnego dla chińskich reform i modernizacji środowiska międzynarodowego[269].

Na tej podstawie ocena chińskiej polityki zagranicznej budzi jednak spore kontrowersje. Z jednej strony Pekin częstokroć odgrywał konstruktywną rolę w stosunkach międzynarodowych, czego przejawem jest m.in. zaangażowanie we współpracę gospodarczą czy aktywność w Radzie Bezpieczeństwa ONZ w kontekście wybranych zagrożeń dla bezpieczeństwa. Z drugiej jednak strony w ostatnich latach można wskazać na szereg przykładów, w których „pokojowa" i „harmonijna" koncepcja aktywności zewnętrznej diametralnie rozmijała

[269] *Chinese Foreign Policy. What Are The Main Tenets Of China's Foreign Policy*? „China Balance Sheet", Center for Strategic & International Studies, s. 1: http://csis.org/files/publication/091019_china-bal_26-Chinese-Foreign-Policy.pdf; dostęp: 13.02.2014.

się z praktyką. Jak zauważył Suisheng Zhao, było to rezultatem przyjętej jeszcze przez Deng Xiaopinga strategii skupienia się na budowie potencjału narodowego na różnych płaszczyznach przy jednoczesnym unikaniu konfrontacji ze Stanami Zjednoczonymi oraz innymi potęgami zachodnimi. Wraz z obiektywnym wzrostem siły i wpływów ChRL jej przywódcy zaczęli jednak uwzględniać w swojej polityce zagranicznej aspekty coraz bardziej kontrowersyjne. Był to główny powód rosnącej asertywności wobec USA na arenie międzynarodowej (Zhao, 2013: 103—105). Na tym tle w stosunkach amerykańsko-chińskich z perspektywy Pekinu zaczęło się z czasem pojawiać coraz więcej problemów. Wśród nich można wymienić m.in. obecność wojskową Stanów Zjednoczonych na Półwyspie Koreańskim i w Japonii, ich wsparcie dla Tajwanu, rywalizację o złoża surowców naturalnych w Afryce, irański program atomowy, a także wspomniane napięcia związane z chińskimi roszczeniami terytorialnymi wobec innych państw Azji Wschodniej (zob. np. Symonides, 2012: 33—58; Matera, 2012: 155—175).

Wszystkie te kwestie wpisywały się w proces rosnącej roli Chin jako przyszłego supermocarstwa i zasadniczego filaru rodzącego się nowego ładu międzynarodowego (zob. np. Hui, 2011; Zhimin, Lulu, 2013). Można się zatem zgodzić z Aleksandrą Łopińską (2012: 109), według której

> rząd w Pekinie, jakkolwiek kontestuje porządek świata, w którym jest miejsce na dyktat wyłącznie jednego mocarstwa, nie zdradza zainteresowania przejęciem w przyszłości roli, którą dzisiaj pełnią Stany Zjednoczone […]. Można przyjąć za pewnik, że Pekin nie jest zainteresowany ochroną istniejącego porządku międzynarodowego w takiej formie, w jakiej oczekuje tego Zachód. W wymiarze politycznym oznaczałoby to bowiem nie tylko konieczność poparcia dla międzynarodowych interwencji w różnych regionach świata, ale również rewizję wewnętrznego porządku w samych Chinach.

W tym kontekście na początku XXI wieku z obu stron zaczęły się pojawiać głosy wskazujące na narastającą „strukturalną" rywalizację między Chinami i Stanami Zjednoczonymi (Zhao, 2013: 109). Jae-Kyung Park wskazał na trzy czynniki determinujące tę sytuację. Po pierwsze wynika to z braku wspólnego wroga, który wymusiłby na obu państwach współpracę. Co prawda takie zagrożenia, jak proliferacja broni atomowej czy terroryzm, są problemem zarówno dla Waszyngtonu, jak i Pekinu, jednak nie na tyle, aby zapobiec ich rywalizacji. Po drugie wraz ze wzrostem potencjału ChRL przepaść między oboma krajami maleje. Zdaniem autora wytwarza to swoiste „napięcie psychologiczne" między potęgą „schodzącą" a „wschodzącą". Po trzecie wreszcie rywalizację obu państw determinuje również odmienna ideologia: komunizm ChRL i liberalna demokracja w USA. Na tej podstawie, jak zauważył Park, konflikt zbrojny jest jednak mało prawdopodobny, chociażby ze względu na posiadanie przez obie

potęgi broni atomowej (Park, 2013: 7—9). Warto również przytoczyć opinię Aarona Friedberga, według którego możliwe są trzy scenariusze rywalizacji amerykańsko-chińskiej. Według pierwszego, jeśli rozwój ChRL napotka przeszkody, to dominacja USA w Azji Wschodniej i na Pacyfiku zostanie utrzymana. Zgodnie z drugim, jeśli rozwój USA napotka problemy, to szanse na hegemonię Chin wzrosną. Według trzeciego, jeśli obydwa mocarstwa pozostaną silne, to należy się liczyć z podziałem ideologicznym na tym obszarze (Haliżak, 2013b: 182).

Jakkolwiek środowisko naukowe w większości podzielało opinię, iż nie istnieje duże ryzyko wybuchu konfliktu zbrojnego na tym obszarze (Symonides, 2012: 57—58; Haliżak, 2013b: 183), należy zauważyć, iż zarówno Chiny, jak i Stany Zjednoczone od lat podejmowały działania przygotowawcze w tym kierunku, identyfikując siebie nawzajem jako głównych rywali. Pekin co prawda stale akcentował defensywny charakter swojej polityki obronnej (Gacek, 2009: 171—172), przeczył temu jednak dynamiczny wzrost wydatków militarnych (w latach 2011—2012 wzrost o ponad 11%)[270]. Ich konsekwencją były zwiększone zakupy nowoczesnego uzbrojenia, które wskazywały na chęć zbliżenia się do potencjału Stanów Zjednoczonych. Świadczyło o tym m.in. wyposażenie chińskiej marynarki wojennej w pierwszy lotniskowiec, rozpoczęcie budowy kolejnego na początku drugiej dekady XXI wieku czy rozwój zdolności niszczenia satelitów na orbicie okołoziemskiej[271]. Działania te były prawidłowo identyfikowane przez stronę amerykańską. Warto tu przytoczyć ustalenia raportu Departamentu Obrony dla Kongresu USA pod tytułem *Military and Security Developments Involving the People's Republic of China 2013*. Stwierdzono tam jednoznacznie, iż ChRL kontynuowała długofalowy program modernizacji swych sił obliczony na zwyciężenie w krótkotrwałym, regionalnym konflikcie zbrojnym o wysokiej intensywności. Według raportu „przygotowywanie się do potencjalnego konfliktu w Cieśninie Tajwańskiej" pozostaje głównym założeniem polityki obronnej Pekinu, choć wraz ze wzrostem pozycji i znaczenia na arenie międzynarodowej coraz bardziej dostosowuje on środki wojskowe do działania poza regionem Azji Wschodniej (*Military and Security Developments*, 2013: i). Mimo tych zabiegów chińscy przywódcy, mając świadomość utrzymywania się nadal ogromnych dysproporcji wojskowych między Stanami Zjednoczonymi a ChRL, szczególny nacisk położyli w okresie pozimnowojennym

[270] *China Raising 2012 Defense Spending to Cope With Unfriendly „Neighborhood"*. Bloomberg, 05.03.2012: www.bloomberg.com/news/2012-03-04/china-says-defense-spending-will-increase-11-2-to-106-4-billion-in-2012.html; dostęp: 13.02.2014.

[271] M. Thompson: *China Doubling Its Aircraft Carrier Fleet*. „Time" 20.01.2014: http://swampland.time.com/2014/01/20/china-doubling-its-aircraft-carrier-fleet; dostęp: 13.02.2014; J. Johanson-Freese: *China's Anti-Satellite Program: They're Learning*. China-US Focus, 12.07.2013: www.chinausfocus.com/peace-security/chinas-anti-satellite-program-theyre-learning; dostęp: 13.02.2014.

na wytworzenie unikalnych zdolności walki asymetrycznej, które pozwoliłyby na zniwelowanie amerykańskiej przewagi jakościowej. Oprócz wspomnianego wyżej potencjału, przydatnego m.in. do niszczenia amerykańskich satelitów, do tej grupy zaliczono również możliwość dokonywania ofensywnych operacji w cyberprzestrzeni[272].

Analizując znaczenie cyberataków w relacjach amerykańsko-chińskich, warto jednak rozpocząć od krótkiego omówienia potencjału obu państw, jeśli chodzi o technologie teleinformatyczne. Z jednej strony, jak wspomniano wcześniej, Stany Zjednoczone były kolebką rewolucji informatycznej, miejscem, gdzie dokonano największych osiągnięć w tej dziedzinie, czego najdonioślejszym symbolem było powstanie Internetu. USA od początku były zatem jednym z globalnych centrów procesów komputeryzacji i informatyzacji, charakteryzujących się wysokim stopniem zaawansowania przyjmowanych rozwiązań w tej dziedzinie. Z pewnością przyczyniło się do tego funkcjonowanie w tym kraju największych i najbardziej zasłużonych ośrodków badawczych, instytucji i przedsiębiorstw zajmujących się rozwojem ICT. Takie korporacje, jak Microsoft, Intel, Google, IBM, Apple Inc., Amazon, HP czy Dell, od dekad wyznaczają najwyższe światowe standardy, zarówno jeśli chodzi o oprogramowanie, sprzęt komputerowy, jak i świadczenie rozmaitych usług online. Do światowej elity należą również korporacje zajmujące się zabezpieczeniami komputerowymi, w tym przede wszystkim Symantec oraz McAfee. Warto jednak zaznaczyć, iż USA, będąc w ścisłej czołówce sektora teleinformatycznego, w *ICT Development Index* z 2011 roku zajmowały dopiero 15. miejsce (*Measuring the Information Society*, 2012: 21). Bez względu na ten fakt Stany Zjednoczone były historycznie jednym z pierwszych państw, które zainteresowały się tematyką cyberbezpieczeństwa. Było to o tyle naturalne, iż większość problemów z nim związanych początkowo występowało właśnie na terytorium USA. Ponadto to Stany Zjednoczone stały się jednym z prekursorów wprowadzania rozwiązań teleinformatycznych w różne dziedziny funkcjonowania administracji publicznej oraz infrastruktury krytycznej. Już w 1995 roku Departament Obrony powołał Zarząd Walki Informacyjnej (Information Warfare Executive Board), który był odpowiedzialny za obronę amerykańskich interesów w cyberprzestrzeni. To właśnie on podjął jedne z pierwszych spójnych prac nad skutkami wrogiej działalności w globalnej sieci w kontekście nowego modelu konfliktów zbrojnych (Lakomy, 2012: 210; Reeder, Chenok, Evans, Lewis, Paller, 2012). Te pierwsze kroki zmierzające do zapewnienia Stanom Zjednoczonym bezpieczeństwa teleinformatycznego były jednak stosunkowo ograniczone. Jak zauważyła Dominika Dziwisz (2011: 107):

[272] S. Kumar: *Asymmetric Capabilities of China's Military*. Institute of Peace and Conflict Studies, 19.11.2008: www.ipcs.org/article/military/asymmetric-capabilities-of-chinas-military-2735.html; dostęp: 13.02.2014.

ataki z 11 września 2001 r. odkryły szereg słabości systemu komunikacji między jednostkami sektora rządowego. Ujawnił się także brak wspólnego planu awaryjnego na wypadek sytuacji kryzysowej. W 2001 r. utworzono więc Departament Bezpieczeństwa Krajowego (Department of Homeland Security, DHS), odpowiedzialny m.in. za przygotowanie ćwiczeń i sprawdzenie gotowości do odparcia ataku z cyberprzestrzeni.

W efekcie utworzono także system analizy, ostrzegania i zarządzania zagrożeniami o znaczeniu narodowym w środowisku cyberprzestrzennym (National Cyberspace Security Response System). Kolejnym krokiem było przyjęcie w lutym 2003 roku *The National Strategy to Secure Cyberspace*, w której uznano zabezpieczenie sieci teleinformatycznych za jedno z najpoważniejszych wyzwań dla Stanów Zjednoczonych. Strategię USA oparto na pięciu filarach: budowie narodowego systemu reagowania na zagrożenia cyberprzestrzenne, wprowadzeniu programu minimalizującego zagrożenia w tej sferze, wprowadzeniu programu edukacyjnego, nowych rozwiązań technologicznych przy zabezpieczaniu rządowych sieci, a także rozwijaniu współpracy zarówno na arenie wewnętrznej, jak i w środowisku międzynarodowym. W międzyczasie sieci komputerowe sektora publicznego i prywatnego USA (w tym rządowe, wojskowe, korporacyjne i uniwersyteckie) stały się jednym z najpopularniejszych celów ataków na świecie (Lakomy, 2011a: 144—150). Do rzeczywistego przełomu w amerykańskiej polityce bezpieczeństwa teleinformatycznego doszło jednak dopiero po 2007 roku w wyniku wydarzeń w Estonii (Lakomy, 2012: 210). Potwierdziły one znaczenie oraz potencjał cyberprzestrzeni jako środowiska, w którym wyrastają nowe wyzwania dla interesów narodowych. Doprowadziło to do wzmożonych działań, których celem było dostosowanie państwa do wymogów środowiska bezpieczeństwa przełomu pierwszej i drugiej dekady XXI wieku. Już w 2008 roku przyjęto inicjatywę CNCI (*Comprehensive National Cybersecurity Initiative*), która skupiała się na trzech założeniach: utworzeniu „wysuniętej linii obrony" wobec najpoważniejszych zagrożeń dla sieci, wzmocnieniu amerykańskich zdolności kontrwywiadowczych oraz zabezpieczeniu pod względem logistycznym kluczowych technologii informacyjnych, a także wzmocnieniu przyszłego środowiska cyberbezpieczeństwa m.in. poprzez działania edukacyjne i badawcze (*Comprehensive National Cybersecurity*, 2008: 1—2). Do kolejnego przełomu w tej dziedzinie doszło dopiero w okresie prezydentury Baracka Obamy, który okazał się pierwszym przywódcą USA przykładającym tak dużą wagę do regulacji tych zagadnień. Jedną z pierwszych podjętych przez niego decyzji było powołanie „cyber cara", czyli urzędu doradcy ds. cyberbezpieczeństwa[273]. Jednocześnie Biały Dom opublikował raport (*Cyberspace Policy*

[273] E. Nakashima: *Obama Set to Create A Cybersecurity Czar With Broad Mandate*. „The Washington Post" 26.05.2009: www.washingtonpost.com/wp-dyn/content/article/2009/05/25/AR2009052502104.html; dostęp: 14.02.2014.

Review), w którym wskazano na najważniejsze priorytety polityki amerykańskiej w tej dziedzinie. Zawarto w nim szereg interesujących stwierdzeń wskazujących na dotychczasowe zaniedbania. Zauważono m.in., iż „naród jest na rozdrożu", a utrzymanie „*status quo* jest nie do zaakceptowania". W związku z tym zaproponowano 10-punktowy plan działań naprawczych, w którym uwzględniono m.in. powołanie doradcy ds. cyberbezpieczeństwa, zintensyfikowanie działań badawczo-rozwojowych w sektorze najnowszych technologii czy stworzenie planu reagowania na incydenty komputerowe (*Cyberspace Policy Review*, 2009: I—VI). Dokument ten świadczył więc z jednej strony o znacznych zapóźnieniach w stosunku do skali wyzwań, przed którymi stały Stany Zjednoczone, z drugiej natomiast był wyrazem wysuwania na pierwszy plan tych kwestii przez administrację Baracka Obamy.

W praktyce wszystkie powyższe działania koncepcyjne na przełomie pierwszej i drugiej dekady XXI wieku przejawiały się dwojako. Po pierwsze w ramach Departamentu Bezpieczeństwa Krajowego utworzono w październiku 2008 roku Narodowe Centrum Integracji Komunikacji i Cyberbezpieczeństwa (National Cybersecurity and Communications Integration Center). Była to działająca przez całą dobę struktura odpowiedzialna za obserwację sieci oraz ostrzeganie przed zagrożeniami narodowej infrastruktury krytycznej[274]. Po drugie bardziej niż dotychczas zaczęto doceniać coraz poważniejsze, polityczne i wojskowe konsekwencje działań w przestrzeni teleinformatycznej. Symbolicznym wyrazem tej świadomości stało się powołanie w czerwcu 2009 roku amerykańskiego dowództwa w cyberprzestrzeni (United States Cyber Command — USCYBERCOM), do którego zadań zaliczono m.in. obronę sieci komputerowych Departamentu Obrony, wspieranie operacji zbrojnych w cyberprzestrzeni oraz przygotowywanie i prowadzenie szerokiego spektrum operacji militarnych w tym środowisku[275]. Świadczyło to więc dobitnie, iż USA uznały cyberprzestrzeń za kolejny, piąty teatr wojny.

Za praktyką tą podążyły inne niezbędne decyzje polityczne. Otóż Waszyngton zdecydował, iż najpoważniejsze cyberataki wymierzone w amerykańskie sieci komputerowe mogą się spotkać z odpowiedzią zbrojną. Świadczyła o tym najdobitniej wspomniana wypowiedź sekretarza obrony Leona Panetty z października 2012 roku, kiedy ostrzegł przed możliwością wystąpienia „cyber Pearl Harbor". Charakteryzując rosnące zagrożenie ze strony innych państw dla amerykańskiej infrastruktury krytycznej, stwierdził, iż Stany Zjednoczone mogą odpowiedzieć konwencjonalnymi siłami zbrojnymi na najgroźniejsze cyberataki. Była to wypowiedź bezprecedensowa, która wskazywała na rosnące znaczenie

[274] *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center*. Office of the Press Secretary. Department of Homeland Security. Washington, D.C. 30.10.2009: www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened; dostęp: 14.02.2014.

[275] *U.S. Army Cyber Command*: www.arcyber.army.mil/org-uscc.html; dostęp: 14.02.2014.

tej problematyki dla amerykańskiej racji stanu[276]. W kolejnych latach politykę tę kontynuowano, czego dowodziło przyjęcie przez administrację Obamy *National Strategy for Trusted Identities in Cyberspace* w kwietniu 2011 roku czy ujawniona decyzja z 2013 roku o powiększeniu USCYBERCOM do pułapu 4000 żołnierzy[277]. Wszystkie te ruchy wskazywały, iż Stany Zjednoczone słusznie były postrzegane jako światowy lider w zakresie zdolności do ofensywnego i defensywnego działania w przestrzeni teleinformatycznej, przeznaczając na ten cel nie tylko znaczne środki finansowe, ale podejmując również pionierskie decyzje polityczne (Dziwisz, 2011: 122; Czebotar, 2013: 65—83; Dziwisz, 2013: 85—97).

Warto również szerzej omówić stosunek Chińskiej Republiki Ludowej do tych zagadnień. Przede wszystkim należy podkreślić, iż pod względem zaawansowania technologicznego na początku drugiej dekady XXI wieku znajdowała się ona daleko w tyle za Stanami Zjednoczonymi. W przytaczanym już wielokrotnie *ICT Development Index* za 2011 rok ChRL zajmowała dalekie 78. miejsce, np. za Jordanią, Wenezuelą czy Trynidadem i Tobago (*Measuring the Information Society*, 2012: 21). Trudno jednak nie docenić dynamiki rozwoju sektora ICT w tym kraju oraz jego potencjału w perspektywie całokształtu globalnej rewolucji informatycznej. Jak zauważyli Xinxiang Chen, Jiaqing Gao oraz Wenda Tan (2005: 27—36), postępy w tej dziedzinie w znacznym stopniu wiązały się z szybkim rozwojem gospodarczym Chin. Świadczył o tym m.in. fakt, iż kraj ten miał w połowie 2013 roku największą liczbę internautów, ocenianą na ok. 591 milionów (*Statistical Report*, 2013: 9). Powstało tam także wiele potężnych korporacji sektora ICT: należy tu wymienić m.in. Baidu (wyszukiwarka internetowa), DXY.cn (media społecznościowe), Neusoft (oprogramowanie) czy Huawei Technologies Co. Ltd. (sprzęt komputerowy i telekomunikacyjny). Warto również zauważyć, iż Chiny stały się globalnym liderem, jeśli chodzi o najpotężniejsze komputery obliczeniowe, przydatne m.in. do łamania szyfrów czy właśnie walki informacyjnej. W 2010 roku superkomputer Tianhe 1A o szybkości ponad 2.5 petaFLOP-ów stał się najszybszym urządzeniem tego typu na świecie. W 2013 roku jego następca Tianhe 2 miał już szybkość ponad 33 petaFLOP-ów, stanowiąc kolejny rekord[278]. Błyskawiczny postęp był więc

[276] E. Bumiller: *Panetta Warns of Dire Threat of Cyberattack on U.S.* „The New York Times" 11.10.2012: www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyber attack.html?pagewanted=all&_r=0; dostęp: 14.02.2014; *Leon Panetta vows retaliation for cyberattack*. Long Island Newsday, 12.10.2012: www.newsday.com/news/nation/leon-panetta-vows-retaliation-for-cyberattack-1.4108337; dostęp: 14.02.2014.

[277] G. Greenwald: *Pentagon's new massive expansion of 'cyber-security' unit is about everything except defense*. „The Guardian" 28.01.2013: www.theguardian.com/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet; dostęp: 14.02.2014.

[278] *Tianhe-1A: National Supercomputing Center in Tianjin*. Top 500 Supercomputer Sites: www.top500.org/featured/systems/tianhe-1a-national-supercomputing-center-in-tianjin/#; dostęp: 14.02.2014; S. Chen: *World's fastest computer Tianhe-2, might get very little use*. „South

ewidentny, mimo że władze ChRL starały się utrzymać ścisłą kontrolę nad rodzimym Internetem. Wskazuje się tu z reguły na dwa rodzaje mechanizmów. Po pierwsze w 1998 roku chińskie Ministerstwo Bezpieczeństwa Publicznego zainicjowało projekt „Złotej Tarczy" (*Golden Shield Project,* określany również jako *Great Firewall of China*). Polegał on na zbudowaniu systemu zapór ogniowych (*firewalls*) oraz serwerów *proxy* w celu zablokowania użytkownikom dostępu do niektórych danych i materiałów w globalnej sieci. Założeniem projektu było powstrzymanie obywateli od działań w cyberprzestrzeni, które mogłyby zaszkodzić bezpieczeństwu narodowemu, ujawnić tajemnice państwowe, naruszyć interesy państwa lub społeczeństwa, a także złamać konstytucję. Po drugie służby ChRL podejmowały inne działania zmierzające do cenzury zawartości Internetu, co przejawiało się to m.in. ręcznym blokowaniem stron internetowych rozmaitych grup opozycyjnych, wrogich rządów i mediów lub materiałów o charakterze religijnym[279].

Na tej podstawie należy zauważyć, iż rząd chiński stosunkowo wcześnie zainteresował się możliwością uzyskania zaawansowanych zdolności do ofensywnego i defensywnego działania w cyberprzestrzeni. Jako moment przełomowy często wskazuje się tu na operację „Pustynna Burza", która uświadomiła decydentom w Pekinie skalę przepaści technologicznej między USA a ChRL (Clarke, Knake, 2010: 47—51). W jej wyniku w połowie lat 90. XX wieku zaczęto przygotowywać nowe rozwiązania koncepcyjne dotyczące konfrontacji ze Stanami Zjednoczonymi. Wei Jincheng opracował np. nowatorski artykuł opublikowany w czasopiśmie wydawanym przez Chińską Armię Narodowo-Wyzwoleńczą, w którym zasugerował wykorzystanie Internetu jako nowej platformy walki zbrojnej. Właśnie taką drogą podążył twórca chińskich zdolności do walki informacyjnej, generał major Wang Pufeng[280]. Zapoczątkowane przez niego wysiłki miały charakter wielowymiarowy i obejmowały zarówno rozbudowę potencjału do działań psychologicznych (PSYOPS), jak i do walki w przestrzeni teleinformatycznej za pomocą wyspecjalizowanych cyberbroni (Lai, Rahman, 2012: 41). Tak uformowane zdolności do walki asymetrycznej miały być wykorzystane na wszystkich teatrach wojny w sposób innowacyjny, zmierzający do zakłócenia funkcjonujących konwencjonalnie systemów i urządzeń. Często koncepcję tę porównywało się do doświadczeń z zakresu wschodnich

China Morning Post" 20.06.2013: www.scmp.com/news/china/article/1264529/worlds-fastest-computer-tianhe-2-might-get-very-little-use; dostęp: 14.02.2014.

[279] Zob. Lewis, 2006; *„Race to the Bottom"*, 2006, s. 9—25; A. August: *The Great Firewall: China's Misguided — and Futile — Attempt to Control What Happens Online*. „Wired" 23.10.2007: www.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all; dostęp: 14.02.2014.

[280] Wang Pufeng (1998: 319) napisał artykuł, w którym stwierdził między innymi, iż Chiny muszą odwołać się do kombinacji walki informacyjnej z maoistowską oraz marksistowską myślą wojskową, aby dostosować się do nowych uwarunkowań na polu walki. Istotą tej myśli miało być pokonanie silniejszego wroga za pomocą środków niekonwencjonalnych.

sztuk walki, w których zwycięstwo zależy od znajomości wrażliwych obszarów organizmu przeciwnika. Czerpiąc z tych wzorców, chińska strategia zakładała dokonywanie uderzeń właśnie w najsłabsze punkty infrastruktury potencjalnego wroga. Przejawem tego było nie tylko wykształcenie zdolności do cyberataków, ale także technologia zakłócania sygnałów GPS, z których korzystają amerykańskie siły zbrojne, czy możliwość niszczenia satelitów znajdujących się na orbicie okołoziemskiej (Ibidem, s. 41—45). O przyjęciu takiego podejścia świadczyło opracowanie z 1997 roku pt. *On Commanding Warfighting under High-Tech Conditions*, opublikowane przez Narodowy Uniwersytet Obrony (PLA National Defence University). Przyrównano tam działania w cyberprzestrzeni do akupunktury, co miało polegać na paraliżowaniu wrażliwych połączeń na styku systemów dowodzenia, kontroli, komunikacji i informacji przeciwnika (Kanwal, 2009: 18). Warto również wspomnieć o artykule Wanga Baocuna oraz Li Fei (1998: 330), w którym do elementów walki informacyjnej zaliczono m.in. wykorzystanie wirusów komputerowych. Kolejnym potwierdzeniem takiego sposobu myślenia była wspólna publikacja dwóch pułkowników chińskiej armii Qiao Lianga oraz Wang Xiangsui pod tytułem *Unrestricted Warfare*. Przyznano w niej, że istnieje możliwość walki z bardziej zaawansowanym technologicznie przeciwnikiem za pomocą środków asymetrycznych. Zawarte tam opinie sugerowały, iż przyszła wojna prowadzona przez ChRL miała polegać właśnie na niekonwencjonalnych atakach wymierzonych we wszystkie elementy składające się na potęgę państwa w płaszczyźnie politycznej, ekonomicznej, militarnej czy informacyjnej. Tego typu optyka była także widoczna w reformach wdrożonych przez chińską armię. Polegały one przede wszystkim na otworzeniu się na rewolucję w sprawach wojskowych (RMA), czego rezultatem było np. dwukrotne zmniejszenie liczby żołnierzy w latach 90. XX oraz daleko idąca komputeryzacja i informatyzacja. Z czasem zaczęto postrzegać te tendencje jako „transformację od walki mechanicznej ery przemysłowej do… wojny decyzji, kontroli, wojny wiedzy oraz wojny intelektu" (Hildreth, 2002:15; Liang, Xiangsui, 1999).

W konsekwencji doprowadziło to do wykształcenia nowatorskiego podejścia do tej problematyki na początku XXI wieku. Określane mianem Zintegrowanej Walki Sieciowo-Elektronicznej (Integrated Network Electronic Warfare — INEW), miało polegać na wykorzystaniu narzędzi komputerowych oraz środków walki elektronicznej przeciwko systemom informacyjnym przeciwnika. Głównym tego celem było zablokowanie mu zdolności zbierania i przetwarzania danych w trakcie konfliktu zbrojnego. Aby osiągnąć takie możliwości, Chińska Armia Ludowo-Wyzwoleńcza zaczęła prowadzić szeroką akcję rekrutacyjną, dzięki której zatrudniono najwybitniejszych krajowych specjalistów z zakresu bezpieczeństwa teleinformatycznego. Ustanowiono ponadto trzy centra szkoleniowe kadry: w akademii w Wuhan, na politechnice w Zhenghou oraz na uniwersytecie w Changshy (Communications Command Academy, Information Engi-

neering University oraz National Defence Science and Technology University). Prowadzono również regularne ćwiczenia wykształcające umiejętności polegające na zbieraniu wrażliwych informacji w cyberprzestrzeni, działaniach propagandowych, cyberobronie lub wprowadzaniu przeciwnika w błąd (*deception*). W efekcie tych przemian w 2003 roku ogłoszono, że Chińska Armia Narodowo-Wyzwoleńcza utworzyła pierwsze jednostki wojskowe przeznaczone wyłącznie do walki informacyjnej[281]. Zdaniem Pentagonu były one odpowiedzialne m.in. za prowadzenie rozpoznania informacyjnego, tworzenie „min" i „bomb" informacyjnych, akcje propagandowe oraz szpiegowskie (Clarke, Knake, 2010: 57—58). Warto zarazem zauważyć, iż na początku XXI wieku Pekin nie zdecydował się na stworzenie odrębnego dowództwa w cyberprzestrzeni wzorem USA, lecz dostosował do funkcjonowania w niej już te istniejące. Według dostępnych danych w ramach sztabu generalnego za aktywność w tym środowisku, a więc obronę własnych sieci, działania cyberszpiegowskie oraz operacje zbrojne, odpowiedzialność przejęły wydziały III oraz IV[282].

Na tle powyższych informacji widać wyraźnie, iż Chińska Republika Ludowa rozmyślnie rozwinęła swój potencjał w tej dziedzinie, który miał stać się jednym z głównych komponentów arsenału asymetrycznych środków powstrzymywania USA na arenie międzynarodowej. Według zachodnich ekspertów dysponuje ona grupą od kilku tysięcy do nawet 180 000 osób działających w sieciach komputerowych (zatrudnionych zarówno przez wojsko, jak i tzw. *freelancerów* wynajmowanych przez władze)[283]. Takie sugestie spotykają się jednak od lat ze sprzeciwem ze strony Pekinu, który w wymiarze deklaratywnym jednoznacznie opowiada się za pokojowym i harmonijnym współistnieniem w cyberprzestrzeni. Warto tutaj przytoczyć słowa chińskiego badacza Li Zhanga (2012: 803—804), który podsumował tę politykę następująco:

> stanowisko Chin polega na tym, że narody na całym świecie powinny pielęgnować wartość cyberprzestrzeni — pierwszej przestrzeni stworzonej przez człowieka — i powinny stanowczo przeciwstawiać się militaryzacji Internetu.

---

[281] Według innych informacji pierwsza chińska jednostka do działań w środowisku informacyjnym powstała już w 2000 roku. Zob. J.M. Spade: *China's Cyber Power and America's National Security*. U.S. Army War College 2011, s. 12—16: www.carlisle.army.mil/dime/documents/China%27s%20Cyber%20Power%20and%20America%27s%20National%20Security%20Web%20Version.pdf; dostęp: 14.02.2014; P. Paganini: *China vs. US, cyber superpowers compared, Infosec Institute*. 10.06.2013: http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared; dostęp: 14.02.2014.

[282] W. Minnick: *China's PLA Involved in Cyber Espionage: Report*. DefenseNews, 10.11.2011: www.defensenews.com/article/20111110/DEFSECT04/111100310/China-s-PLA-Involved-in-Cyber-Espionage-Report; dostęp: 14.02.2014.

[283] Za: H. Jones: *China's „Cyberwar" Against the US: Truth or Fiction*? University of Cambridge, 23.07.2013: www.pem.cam.ac.uk/wp-content/uploads/2013/04/Hattie-Jones-Cyber-Warfare-Essay.pdf; dostęp: 17.02.2014.

> Chiny wspierają pokojowe wykorzystanie cyberprzestrzeni. Zajmują stanowisko „*no first use*" cyberbroni, jak również nieatakowania obiektów cywilnych. Jednak ze względu na kompleksowość tego wzajemnie połączonego systemu trudno nakreślić precyzyjną linię pomiędzy sieciami cywilnymi i wojskowymi […]. Poglądy Chin polegają na tym, że obecna Karta Narodów Zjednoczonych oraz wszystkie istniejące prawa konfliktów zbrojnych obowiązują w cyberprzestrzeni — w szczególności zasada zakazu użycia siły oraz pokojowego regulowania międzynarodowych sporów.

Jednocześnie jednak autor zaznaczył, że ChRL wierzy w możliwość aktualizacji istniejących zasad prawa międzynarodowego w taki sposób, aby lepiej odpowiadały specyfice tej domeny.

W świetle powyższych tendencji nie dziwi więc fakt, iż narastająca rywalizacja amerykańsko-chińska na arenie międzynarodowej przeniosła się również w wymiar cyberprzestrzenny. Pierwszy incydent, który świadczył o zapoczątkowaniu tego procesu, miał miejsce już w 1999 roku[284] w trakcie natowskiej interwencji w Kosowie. Gdy w maju tego roku samoloty amerykańskie zniszczyły ambasadę ChRL w Belgradzie, doszło do masowego cyberataku na USA, który został przeprowadzony równolegle na kilku wektorach. Po pierwsze odwołano się do metody DDoS w celu zablokowania witryny Białego Domu (www.whitehouse.gov), która w efekcie przestała funkcjonować aż na trzy dni. Po drugie na adresy poczty elektronicznej administracji USA zaczęto masowo wysyłać spam z zamiarem jej sparaliżowania. Po trzecie włamano się na strony internetowe Departamentu Energii oraz Departamentu Spraw Wewnętrznych (Department of Interior). Dokonano dzięki temu standardowego *web defacement*, zamieszczając tam ostre antyamerykańskie, antynatowskie i antywojenne hasła typu*: Protest USA's Nazi action! Protest NATO's brutal action!* Do odpowiedzialności za ataki przyznało się wiele chińskich grup haktywistycznych, w tym m.in. Hong Kong Danger Duo czy Javaphile[285]. Reakcja władz ChRL okazała się bardzo pozytywna: po tym, jak i innych ówczesnych incydentach (np. w 1999 roku na tle wypowiedzi prezydenta Tajwanu Lee Tenga-hui) Pekin gratulował sprawcom udanych operacji w cyberprzestrzeni (Krekel, 2009: 36—37).

Do następnego starcia online doszło już w kwietniu i maju 2001 roku na tle wzrostu napięcia politycznego i militarnego między Chinami a USA, do czego doprowadziło zderzenie w powietrzu chińskiego myśliwca J-8 z amerykańskim samolotem zwiadowczym EP-3 nad Morzem Południowochińskim (Kan, 2001). Tym razem miały one charakter obustronny, amerykańscy haktywiści w reak-

[284] Już wcześniej Chiny, a w zasadzie społeczność hakerska ChRL skupiona wokół China Hacker Emergency Meeting Center, wykazywała znaczną aktywność na arenie międzynarodowej. Przykładem były ataki przeciwko rządowi Indonezji w 1998 roku. Zob. Carr, 2010: 2.

[285] E. Messmer: *Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says*. CNN, 12.05.1999: http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg; dostęp: 17.02.2014; Pandey, 2010, s. 6.

cji na ten incydent zaatakowali bowiem około 1000 chińskich stron internetowych, a w odpowiedzi, w maju 2001 roku, grupa Honker Union of China dokonała cyberataku na taką samą liczbę amerykańskich witryn, w tym m.in. Białego Domu, która została zablokowana metodą DDoS na ok. 2 godziny. Tym razem reakcja Pekinu była już inna, aktywność chińskich haktywistów oceniono bowiem jako przejaw „web-terroryzmu" oraz złamanie prawa. Cofnięcie poparcia dla tych grup na początku XXI wieku doprowadziło w efekcie do przekształcenia znacznej ich części w niezależne spółki zajmujące się bezpieczeństwem teleinformatycznym. Ze względu na stopień kontroli władz nad krajowym Internetem bez ich zgody jakakolwiek działalność tego typu nie mogła mieć miejsca. Wielu przedstawicieli tego środowiska nawiązało zatem bliskie kontakty z chińskim rządem. Przykładowo można tu wymienić członków takich grup, jak The Patriot Hackers, The Black Eagle czy Green Army Alliance. Jakkolwiek oficjalnie władze w Pekinie odcinały się od tych związków, to, jak udowodniły późniejsze badania, na początku XXI wieku cyberataki prowadzone z terytorium ChRL przeciwko amerykańskim sieciom komputerowym szeroko korzystały ze złośliwego oprogramowania i technik opracowanych pierwotnie przez chińskie podziemie hakerskie i haktywistyczne (Krekel, 2009: 37—38).

Powyższy zwrot w polityce ChRL na początku wieku wynikał z faktu, iż już wtedy rozpoczęła się prawdopodobnie nowatorska kampania w cyberprzestrzeni, która w odróżnieniu od wcześniejszych incydentów miała zupełnie inny charakter. Jej celem było skryte pozyskiwanie z amerykańskich serwerów i sieci niejawnych danych, przede wszystkim dotyczących potencjału wojskowego USA oraz najnowszych technologii. Wykorzystano do tego niewykrywalne wówczas programy typu trojan. Od 2002 lub 2003 roku włamano się m.in. do komputerów Departamentu Obrony, Departamentu Stanu, Departamentu Energii, Departamentu Bezpieczeństwa Krajowego oraz największych korporacji, głównie tych współpracujących z armią (np. Lockheed Martin). Ponadto zaatakowano szereg innych struktur wchodzących w skład US Army oraz NASA[286]. Przez wiele miesięcy dokonywano wielokrotnych i — co najważniejsze — niewykrytych penetracji, w których wyniku utracono wiele bezcennych informacji, m.in. dotyczących technologii, których USA nie udostępniają partnerom zagranicznym. W ten sposób chińscy specjaliści przejęli m.in. oprogramowanie wykorzystywane w amerykańskich myśliwcach (Falconview 3.2), plany napędów kosmicznych czy paneli słonecznych dla Mars Reconaissance Orbiter. Cała kampania, określona mianem *Titan Rain*, została ujawniona opinii publicznej dopiero w 2005 roku przez magazyn „Time". Warto dodać, iż zidentyfikowane adresy IP sprawców wskazywały na ich lokalizację w prowincji Guangdong w Chinach. Więk-

[286] Można tu wymienić m.in. U.S. Army Information Systems Engineering Command, Defense Information Systems Agency, Naval Ocean System Center czy U.S. Army Space and Strategic Defense.

szość ekspertów uznała te incydenty za przejaw działalności służb specjalnych ChRL, w ten sposób interpretował je chociażby dyrektor SANS Institute Alan Paller. Przedstawiciele władz w Pekinie odrzucili jednak wszelkie zarzuty w tej sprawie[287].

Po raz kolejny znaczenie cyberprzestrzeni w stosunkach amerykańsko-chińskich wzrosło w 2006 roku. Pod koniec maja do jednego z pracowników Departamentu Stanu trafiła wiadomość e-mail z zainfekowanym trojanem plikiem Microsoft Word. Pozwoliło to uzyskać sprawcom krótkotrwały dostęp do sieci rządowej Stanów Zjednoczonych za pomocą stworzonego *backdoora*. Został on wykryty przez służby i usunięty. Jak się jednak szybko okazało, w trakcie rutynowej kontroli natrafiono na kolejne metody naruszenia integralności i bezpieczeństwa danych w systemach teleinformatycznych władz USA. Odkryto m.in. nieznany dotychczas *exploit* w systemach Microsoftu (Reid, 2007). Choć nie ujawniono niezbitych dowodów w tej sprawie, incydent ten był powszechnie postrzegany jako przejaw rosnącej aktywności Pekinu w cyberprzestrzeni[288].

W sierpniu 2006 roku Pentagon ujawnił swoją kolejną porażkę w tej dziedzinie, która dotyczyła utraty danych z wojskowej sieci NIPRNET. Zdaniem jego przedstawicieli wrogie, cywilne grupy „hakerów" działających z terytorium Chińskiej Republiki Ludowej wyprowadziły z niej około 20 terabajtów danych (Mulvenon, 2013: 1). Natomiast w listopadzie tego roku chińscy specjaliści zaatakowali komputery należące do jednej z wyższych szkół wojskowych (US Naval War College), co doprowadziło do odłączenia na pewien czas jej poczty elektronicznej oraz sieci i poskutkowało podniesieniem alarmu przez amerykańskie Dowództwo Strategiczne (U.S. Strategic Command) dla 12 000 wojskowych sieci komputerowych oraz ok. 5 mln komputerów. Jeden z profesorów Naval War College, gen. Richard Goetze, oskarżył o ich zorganizowanie chińskie służby specjalne, podobnego zdania byli również eksperci SANS Institute[289]. Warto również wspomnieć o incydentach, które miały miejsce w kwietniu i maju 2007 roku. W kwietniu zdecydowano o wyłączeniu na kilka miesięcy części sieci komputerowych Departamentu Handlu (należących do Biura Bezpieczeństwa Przemysłowego — Bureau of Industrial Security), natomiast w maju zaatakowano sieci Narodowego Uniwersytetu Obrony (National Defense University). W obu przypadkach służby nie były jednak w stanie zidentyfiko-

[287] Thornburgh, 2005; Carr, 2010: 4—5; N. Thornburgh: *Inside Chinese Hack Attack*. „Time" 25.08.2005: http://content.time.com/time/nation/article/0,8599,1098371,00.html; dostęp: 17.02.2014; T. Espiner: *Security experts lift lid on Chinese hack attacks*. ZDNet, 23.11.2005: www.zdnet.com/security-experts-lift-lid-on-chinese-hack-attacks-3039237492; dostęp: 17.02.2014.

[288] R. Kesselman: *Intel Brief: Chinese cyberwarfare*. ISN ETH Zurich, 11.01.2008: www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=54008; dostęp: 17.02.2014.

[289] *Chinese hackers prompt Navy college site closure*. „The Washington Times" 30.11.2006: www.washingtontimes.com/news/2006/nov/30/20061130-103049-5042r/?page=all; dostęp: 17.02.2014.

wać sprawców[290]. Niemniej wszystkie te wydarzenia, mające wyraźnie charakter cyberszpiegowski, obliczony na wyprowadzenie jak największej ilości wrażliwych danych z komputerów i sieci amerykańskich, doprowadziły do pierwszych oficjalnych reakcji Waszyngtonu. W marcu 2007 roku ówczesny wiceprzewodniczący Kolegium Połączonych Szefów Sztabów USA, gen. James Cartwright, stwierdził jednoznacznie, iż Chiny są zaangażowane w działalność „rozpoznawczą" sieci amerykańskich agencji rządowych oraz korporacji (Mulvenon, 2013: 1).

W 2008 roku tendencje te uległy dalszemu natężeniu. W maju pojawiła się w mediach informacja o możliwym zainfekowaniu złośliwym oprogramowaniem komputera przenośnego amerykańskiego sekretarza ds. handlu Carlosa M. Gutierreza w trakcie jego wizyty w Chinach. Zawartość notebooka miała wówczas zostać skopiowana i wykorzystana do ataku na sieć Departamentu Handlu[291]. Między kwietniem a październikiem 2008 roku pojawiły się z kolei doniesienia portalu Wikileaks o włamaniach do intranetu amerykańskiego Departamentu Stanu. W ich wyniku sprawcy mieli skopiować ok. 50 megabajtów wiadomości e-mail wraz z załącznikami, a także listę nazw użytkownika i haseł do sieci jednej z agencji rządowych. Zgodnie z opublikowanymi przez ten serwis dokumentami odpowiedzialność za te wydarzenia miał ponosić III wydział chińskiego sztabu generalnego. W czerwcu 2008 roku zaatakowano komputery znajdujące się w biurach kilku amerykańskich kongresmanów. Co prawda nie wykryto wówczas sprawców, lecz na ich tożsamość wskazywał fakt, iż część z parlamentarzystów była zaangażowana w walkę o przestrzeganie praw człowieka w Tybecie. Warto także wspomnieć o cyberatakach na bazy danych prezydenckich kampanii wyborczych Republikanów i Demokratów w lecie 2008 roku[292]. Również i w tym wypadku głównymi podejrzanymi były osoby posiadające adresy IP zlokalizowane na terytorium Chińskiej Republiki Ludowej[293].

Przełomowe odkrycia wyjaśniające specyfikę chińskiej aktywności cyberszpiegowskiej poczyniono w 2009 roku, kiedy zespół kanadyjskich badaczy pod kierunkiem Rona Deiberta z uniwersytetu w Toronto oraz Rafala Rohozinsky'ego z The SecDev Group opublikował raport *Tracking Gh0stNet.*

---

[290] *Significant Cyber Incidents Since 2006*. Center for Strategic & International Studies, 30.01.2014: http://csis.org/files/publication/120806_Significant_Cyber_Incidents_Since_2006_0.pdf; dostęp: 17.02.2014.

[291] *U.S. probes whether laptop copied on China trip.* USA TODAY, 29.05.2008: http://usatoday30.usatoday.com/news/nation/2008-05-29-US-china-laptop-copied_N.htm; dostęp: 17.02.2014.

[292] *Significant Cyber Incidents Since 2006*. Center for Strategic & International Studies, 30.01.2014, s. 3: http://csis.org/files/publication/120806_Significant_Cyber_Incidents_Since_2006_0.pdf; dostęp: 17.02.2014.

[293] L. Glendinning: *Obama, McCain computer 'hacked' during election campaign*. „The Guardian" 07.11.2008: www.theguardian.com/global/2008/nov/07/obama-white-house-usa; dostęp: 17.02.2014.

Investigating a Cyber Espionage Network. Ujawniono w nim kampanię cyberataków o podłożu wywiadowczym przeciwko 1295 komputerom znajdującym się aż w 103 krajach. Wykorzystując trojana typu *gh0st RAT*, sprawcy działający z wyspy Hainan w ChRL byli w stanie zaatakować m.in. komputery ministerstw spraw zagranicznych Iranu, Bangladeszu, Łotwy, Indonezji, Filipin, Brunei, Barbadosu czy Bhutanu, ambasad Indii, Korei Południowej, Indonezji, Rumunii, Cypru, Malty, Tajlandii, Tajwanu, Portugalii, Niemiec i Pakistanu, Sekretariatu Stowarzyszenia Narodów Azji Południowo-Wschodniej (ASEAN), Południowoazjatyckiego Stowarzyszenia Współpracy Regionalnej (SAARC), Azjatyckiego Banku Rozwoju (Asian Development Bank), Kwatery Głównej NATO, a także wybranych mediów.

Zdaniem kanadyjskich ekspertów ok. 30% zainfekowanych komputerów miało istotne znaczenie polityczne, gospodarcze, dyplomatyczne czy wojskowe. Chińscy specjaliści dokonywali ataków głównie za pomocą metod *spear-phishingu*, co pozwalało na zarażenie precyzyjnie wybranych jednostek trojanem, a następnie przejęcie nad nimi kontroli. Zastosowane złośliwe oprogramowanie pozwalało m.in. na aktywowanie podłączonych mikrofonów i kamer internetowych, co ułatwiało zbieranie danych także w bezpośrednim otoczeniu komputerów, w tym np. w sekretariacie Dalajlamy. Warto zauważyć, iż poza identyfikacją adresu IP osób kontrolujących sieć szpiegowską *Gh0stNet* autorzy nie stwierdzili jednoznacznie, kto stał za tą operacją (zob. Deibert, Rohozinski, 2009). Wybrane cele (w tym np. tybetańska opozycja), a także sposób działania, jednoznacznie wskazywały przy tym na pośredni lub bezpośredni udział służb specjalnych ChRL. *Casus* ten, jakkolwiek nie dotyczył bezpośrednio stosunków amerykańsko-chińskich, udowodnił skalę działań wywiadowczych podejmowanych przez Chiny w cyberprzestrzeni.

Ten sam zespół badaczy w kwietniu 2010 roku opublikował kolejny raport poświęcony chińskiej aktywności cyberszpiegowskiej: *Shadows in the Cloud: Investigating Cyber Espionage 2.0* (zob. Deibert, Rohozinski, 2010). Omówiono w nim główne sposoby cyberataków, które zastosowano m.in. przeciwko ambasadom Indii oraz Pakistanu w Stanach Zjednoczonych. Sprawcy dzięki metodom *phishingu* oraz trojanom byli w stanie przejąć informacje dotyczące np. aktywności hinduskiej misji dyplomatycznej w Afganistanie. Użyty system kontroli i dowodzenia (C&C) w dużej mierze opierał się na potencjale mediów społecznościowych oraz popularnych serwisów, takich jak Twitter, Google, Blogspot, Baidu czy Yahoo! Mail. Tym razem autorzy raportu więcej miejsca poświęcili sprawcom incydentów. Po pierwsze zauważono, że stały za nimi prawdopodobnie dwie osoby zamieszkałe w Chengdu w ChRL. Po drugie zadano pytanie, czy rząd chiński zamierzał zlikwidować nową sieć szpiegowską Shadow. Według dokumentu brak reakcji mógłby być potwierdzeniem, iż Pekin przychylnie spoglądał na tego typu inicjatywy oraz czerpał z nich określone korzyści. Na tym tle warto zauważyć, iż nie pojawiły się żadne publicznie dostępne informacje świadczące o tym,

iż Chiny przeciwdziałały funkcjonowaniu odkrytej w 2010 roku siatki szpiegowskiej.

Równolegle z omówionymi wyżej opracowaniami doszło do kolejnych poważnych incydentów teleinformatycznych w samych Stanach Zjednoczonych. 21 kwietnia 2009 roku w mediach pojawiła się informacja na temat włamania do części komputerów Pentagonu, w którego wyniku pozyskano dane na temat najdroższego amerykańskiego programu zbrojeniowego w historii Joint Strike Fighter. Sprawcy działający z terytorium Chin byli w stanie skopiować aż kilka terabajtów materiałów na ten temat. Dostęp do sieci Pentagonu uzyskano w podobny sposób, jak miało to miejsce w przypadku robaka *Stuxnet*: zainfekowano komputery przedsiębiorstw zewnętrznych pracujących przy projekcie samolotu F-35. Przy okazji ujawniono, że program JSF był obiektem ataków cyberszpiegowskich już od 2007 roku. O wysokim stopniu zorganizowania całej operacji mógł świadczyć fakt, iż śledczym nie udało się do końca odpowiedzieć na pytanie, jakie informacje utracono. Wynikało to z faktu, iż sprawcy zastosowali zaawansowane szyfrowanie przesyłanych plików. W tym kontekście warto przywołać reakcję ambasady ChRL w Waszyngtonie, która stwierdziła, iż Pekin jest przeciwny wszelkim formom cyberprzestępczości, a zarzuty dotyczące jego działalności cyberszpiegowskiej zostały spreparowane w taki sposób, aby wzbudzić poczucie zagrożenia ze strony Chin[294]. Informacje te były o tyle istotne, iż wpisywały się w coraz bardziej wyraźne sygnały wykradania za pomocą włamań komputerowych najnowszych, cywilnych i wojskowych technologii amerykańskich. Mogły być one w zamyśle sprawców użyte do zasypania przepaści w potencjałach militarnych między oboma państwami. W tym wypadku było to tym bardziej ewidentne, iż Chiny od lat prowadziły własny program myśliwca nowej generacji typu *stealth* J-20[295]. Na tym tle już w maju 2009 roku ujawniono kolejny poważny atak teleinformatyczny, tym razem na amerykański Departament Bezpieczeństwa Krajowego. Włamano się wówczas do Sieci Informacyjnej Bezpieczeństwa Krajowego (Homeland Security Information Network), która była platformą wymiany danych między instytucjami publicznymi różnego szczebla. Tym razem nie ujawniono jednak lokalizacji adresów IP sprawców[296].

Powyższe incydenty nie miały jednak większego znaczenia w świetle poważnej kampanii cyberataków, określonej kryptonimem *Aurora*, która rozpoczęła się w połowie 2009 roku. Została ona wymierzona w naj-

[294] S. Gorman, A. Cole, Y. Dreazen: *Computer Spies Breach Fighter-Jet Project*. „The Wall Street Journal" 21.04.2009: http://online.wsj.com/news/articles/SB124027491029837401; dostęp: 19.02.2014.

[295] *Chengdu J-20 Multirole Stealth Fighter Aircraft, China*. Airforce Technology: www.airforce-technology.com/projects/chengdu-j20; dostęp: 19.02.2014.

[296] B. Bain: *Information-sharing platform hacked*. FCW.com, 13.05.2009: http://fcw.com/articles/2009/05/13/web-dhs-hsin-intrusion-hack.aspx; dostęp: 19.02.2014.

większe amerykańskie korporacje działające głównie w sektorze IT. Do momentu jej ujawnienia w styczniu 2010 roku włamano się m.in. do sieci: Google (wyszukiwarki internetowe, oprogramowanie, reklamy online), Adobe Systems (aplikacje użytkowe), Juniper Networks (urządzenia sieciowe), Rackaspace (hosting), Yahoo! (portale i wyszukiwarki internetowe), Symantec Corporation (oprogramowanie antywirusowe), Northrop Grumman (technologie kosmiczne i obronne), Morgan Stanley (usługi finansowe) czy Dow Chemical Company (przemysł chemiczny). Według doniesień medialnych kampania objęła ponad 30 amerykańskich korporacji[297]. Szkody poniosły również instytucje w innych krajach, w tym m.in. w Niemczech, Wielkiej Brytanii czy na Tajwanie. Komputery z aż 22 państw (w tym także z ChRL) kontaktowały się z serwerami kontroli i dowodzenia[298]. Cała operacja została ujawniona przez korporację Google 12 stycznia 2010 roku. W specjalnym wpisie na jej blogu stwierdzono, iż w wyniku cyberataku pochodzenia chińskiego doszło do naruszenia praw własności intelektualnej, czyli innymi słowy utraty wrażliwych danych. Zdaniem autora wiadomości, Davida Drummonda, w przypadku Google sprawcom chodziło przede wszystkim o uzyskanie dostępu do skrzynek poczty elektronicznej należących do chińskich obrońców praw człowieka. W efekcie doprowadziło to do zaostrzenia polityki tej korporacji wobec Pekinu[299]. Warto zauważyć, iż w *Aurorze* wykorzystano bardzo zaawansowane techniki włamań. Z jednej strony zastosowano *exploit* dnia zerowego znajdujący się w programie Internet Explorer korporacji Microsoft, z drugiej użyto trojana *Hydraq*, który był wcześniej nieznany, a co za tym idzie niewykrywalny dla oprogramowania antywirusowego. Wraz z wejściem na zainfekowaną stronę internetową komputer sam ściągał złośliwy program, który następnie mógł być użyty do dalszej penetracji systemu oraz skopiowania zawartości dysku twardego[300]. Wszystkie zebrane dane były następnie szyfrowane i wysyłane z powrotem do Chin, co pozwalało uniknąć wykrycia konwencjonalnymi metodami. Można się więc zgodzić z przedstawicielem McAfee Labs, który stwierdził, że jeszcze nigdy w historii USA, nie licząc przemysłu obronnego, nie doszło do tak zaawan-

[297] Zob. L. Latif: *HBGary email leak claims Morgan Stanley was hacked*. „The Inquirer" 01.03.2011: www.theinquirer.net/inquirer/news/2029754/hbgary-email-leak-claims-morgan-stanley-hacked; dostęp: 19.02.2014; A. Eunjung Cha, E. Nakashima: *Google China cyberattack part of vast espionage campaign, experts say*. „The Washington Post" 14.01.2010: www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html; dostęp: 19.02.2014.

[298] *The Command Structure of the Aurora Botnet*. Damballa 2010: www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf; dostęp: 19.02.2014.

[299] D. Drummond: *A new approach to China*. Google Blog, 12.01.2010: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html; dostęp: 19.02.2014.

[300] R. Varma: *Combating Aurora*. McAfee Labs: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/67000/KB67957/en_US/Combating%20Threats%20-%20Operation%20Aurora.pdf; dostęp: 19.02.2014.

sowanej serii ataków wymierzonych w komercyjne korporacje, co zupełnie zmieniało postrzeganie zagrożeń teleinformatycznych[301].

Ze względu na skalę tej operacji po raz pierwszy incydenty wywołały ostrą reakcję amerykańskiej dyplomacji. Początkowo sekretarz stanu Hillary Clinton wezwała jedynie ChRL do złożenia wyjaśnień w tej sprawie[302]. Niedługo później zaostrzono stanowisko, czego wyrazem była wypowiedź Clinton z 22 stycznia 2010 roku: „Oczekujemy od władz chińskich dokładnego śledztwa [w sprawie — M.L.] tych cyberwtargnięć […]. Oczekujemy także, iż to śledztwo, a także jego rezultaty będą transparentne"[303]. Ostra jak na dotychczasową praktykę reakcja Waszyngtonu nie wywołała jednak większego odzewu po drugiej stronie Pacyfiku. Wiceminister spraw zagranicznych ChRL He Yafei zbagatelizował te słowa, twierdząc, iż sprawa korporacji Google w żadnym razie nie powinna być łączona ze stosunkami amerykańsko-chińskimi. W przeciwnym wypadku, zdaniem przedstawiciela władz w Pekinie, nastąpiłaby „nadinterpretacja" tych wydarzeń[304]. W tym kontekście należałoby dodać, iż w 2012 roku korporacja Symantec opracowała raport, w którym uznała, iż jednym z odpowiedzialnych za operację *Aurora* była chińska grupa Elderwood. W kolejnych latach miała ona prowadzić inne cyberataki zmierzające do pozyskania tajnych danych oraz technologii (O'Gorman, McDonald, 2012). Powstało jednak pytanie, czy była ona w jakimś stopniu powiązana ze służbami ChRL. Na ich akceptację bądź udział w tych działaniach zdawały się wskazywać trzy fakty. Po pierwsze świadczyła o tym wspomniana już niechęć Pekinu do niezależnych „wojen hakerskich" z przełomu wieków, po drugie fakt, iż rząd chiński posiadał znaczną kontrolę nad rodzimymi użytkownikami Internetu, po trzecie — nie podjęto żadnych wysiłków, aby zablokować kolejne przedsięwzięcia tego typu.

Sprawa operacji *Aurora* bynajmniej nie zakończyła kampanii poważnych cyberataków wymierzonych w żywotne z punktu widzenia amerykańskiej racji stanu podmioty i instytucje. W połowie 2011 roku Google ujawniło próby włamań do skrzynek poczty elektronicznej należących m.in. do przedstawicieli instytucji rządowych USA. Ich sprawcy zostali zlokalizowani w prowincji Shandong w Chinach. Pod koniec maja doszło również do uzyskania nielegalnego dostępu do serwerów korporacji Lockheed Martin. Tym razem jednak poniesione szkody okazały się minimalne. Zbiegło się to w czasie ze wspomnianymi

[301] K. Zetter: *Google Hack Attack Was Ultra Sophisticated, New Details Show*. „Wired" 14.01.2010: www.wired.com/threatlevel/2010/01/operation-aurora; dostęp: 19.02.2014.

[302] B. Johnson: *US asks China to explain Google hacking claims*. „The Guardian" 13.01.2010: www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us; dostęp: 19.02.2014.

[303] C. Kang: *Hillary Clinton calls for Web freedom, demands China investigate Google attack*. „The Washington Post" 22.01.2010: www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html; dostęp: 19.02.2014.

[304] Ibidem.

już zapowiedziami przedstawicieli amerykańskich władz, którzy zadeklarowali, iż mogą traktować najpoważniejsze cyberataki jako akt wojny[305]. W lipcu 2011 roku Departament Obrony USA ujawnił z kolei, że kilka miesięcy wcześniej (w marcu) miał miejsce jeden z najpoważniejszych w historii ataków komputerowych wymierzonych w korporacje sektora obronnego. W jego wyniku utracono ok. 24 000 plików. Zastępca sekretarza obrony William Lynn wyraził wówczas przekonanie, iż włamanie zorganizowały obce służby wywiadowcze, dając tym samym do zrozumienia, iż chodziło o Chińską Republikę Ludową[306]. We wrześniu natomiast wykryto złośliwe oprogramowanie (typu *keylogger*) w komputerach Creech Air Force Base w Newadzie, odpowiedzialnych m.in. za kontrolę dronów operujących nad Afganistanem. Co prawda nieznani sprawcy nie poczynili żadnych nieodwracalnych szkód, mogli jednak uzyskać informacje na temat sposobów działania amerykańskiej floty samolotów bezzałogowych[307]. Ponadto w grudniu 2011 roku ujawniono wcześniejszy incydent (z 2010 roku), do którego doszło w systemach amerykańskiej Izby Handlowej (U.S. Chamber of Commerce) dzięki zastosowaniu metod z zakresu *spear-phishingu*. Według pierwszych doniesień medialnych sprawcy operujący z terytorium Chin zdobyli wówczas wiadomości dotyczące działań lobbystycznych izby w Kongresie, a także wrażliwe dane na temat 3 milionów jej członków. Jak podał „The Wall Street Journal", włamanie miało objąć w sumie ok. 300 komputerów. Później okazało się jednak, że wykradziono pliki jedynie z czterech z nich, należących do ekspertów izby zajmujących się problematyką azjatycką. Mimo to Tom Kellermann z Center for Strategic & International Studies uznał, że cyberatak nosił wszelkie znamiona chińskiego szpiegostwa gospodarczego. Warto dodać, iż paradoksalnie Izba Handlowa wcześniej słynęła z ostrej krytyki polityki cyberbezpieczeństwa Stanów Zjednoczonych, uznając ją za zbyt restrykcyjną[308].

[305] Zob. C. Arthur: *Google phishing: Chinese Gmail attack raises cyberwar tensions*. „The Guardian" 01.06.2011: www.theguardian.com/technology/2011/jun/01/google-hacking-chinese-attack-gmail; dostęp: 19.02.2014; *US defence firm Lockheed Martin hit by cyber-attack*. BBC News, 30.05.2011: www.bbc.co.uk/news/world-us-canada-13587785; dostęp: 19.02.2014.

[306] C. Lefkow: *24,000 files stolen from defense contractor: Pentagon*. Google, 17.07.2011: www.google.com/hostednews/afp/article/ALeqM5gEdFG5Pj-_A4uKTY_ITXq9_bwgWg?docId=CNG.7aa9abffca24b9b885339c57148d2d7d.381&hl=en; dostęp: 19.02.2014.

[307] N. Shachtman: *Exclusive: Computer Virus Hits U.S. Drone Fleet*. „Wired" 07.10.2011: www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet; dostęp: 19.02.2014.

[308] N. Perlroth: *Hacked Chamber of Commerce Opposed Cybersecurity Law*. Bits, 21.12.2011: http://bits.blogs.nytimes.com/2011/12/21/hacked-chamber-of-commerce-opposed-cybersecurity-law/?_php=true&_type=blogs&_r=0; dostęp: 21.02.2014; *Chinese group hacks into US Chamber of Commerce networks*. „Infosecurity Magazine" 22.12.2011: www.infosecurity-magazine.com/view/22834/chinese-group-hacks-into-us-chamber-of-commerce-networks; dostęp: 21.02.2014; W. Shington: *China hackers breached U.S. Chamber of Commerce: report*. Reuters, 21.12.2011: www.reuters.com/article/2011/12/21/us-usa-china-hacking-idUSTRE7BK0J620111221; dostęp: 21.02.2014; H. Tsukayama: *China hack of Chamber of Commerce highlights 'spear-phishing' dangers*. „The Washington Post" 21.12.2011: www.washingtonpost.

Można również wspomnieć o informacji podanej przez NASA, według której w 2011 roku aż 13-krotnie dochodziło do zakończonych sukcesem penetracji jej wewnętrznych sieci komputerowych. Przynajmniej jeden z tych incydentów, który miał miejsce w listopadzie, pochodził z terytorium ChRL. Miał on wyjątkowo poważny charakter, utracono bowiem wówczas kontrolę administracyjną nad częścią intranetu agencji[309].

W 2011 roku korporacja McAfee Labs opublikowała również dwa bardzo ważne raporty na temat chińskiej działalności cyberszpiegowskiej. Pierwszy z nich, przygotowany w lutym, dotyczył rozpoczętej w listopadzie 2009 roku operacji określonej jako *Night Dragon*, wymierzonej w globalną infrastrukturę energetyczną, w tym przede wszystkim w przedsiębiorstwa naftowe, gazowe oraz petrochemiczne. Nie zdecydowano się ujawnić, które dokładnie zostały zaatakowane. Według raportu sprawcy odwoływali się do szerokiej gamy metod, w tym m.in.: *spear-phishingu*, wykorzystywania luk w oprogramowaniu Microsoftu (Windows, Microsoft Active Directory), *SQL injection*, a także instrumentów zdalnej administracji (RAT — Remote Administration Tools) oraz trojanów. Działając głównie z terytorium Chin (miasto Heze w prowincji Shandong), byli oni w stanie uzyskać informacje dotyczące m.in. dokonywanych przez te przedsiębiorstwa operacji finansowych (*Global Energy Cyberattacks*, 2011).

W drugim raporcie z połowy 2011 roku ujawniono kolejną chińską operację cyberszpiegowską o kryptonimie *Shady RAT*. Już we wstępie do tego dokumentu jego autor, Dmitri Alperovitch, stwierdził, iż jest przekonany o tym, że niemal wszystkie wielkie przedsiębiorstwa ze wszystkich sektorów gospodarki albo zostały już zaatakowane w cyberprzestrzeni, albo też niedługo będą. W opracowaniu McAfee Labs ujawniono, iż *Shady RAT* rozpoczęła się jeszcze w połowie 2006 roku, a w jej wyniku wykradziono petabajty danych. Po uzyskaniu dostępu do jednego z serwerów dowodzenia i kontroli ekspertom korporacji udało się zrozumieć podstawowe zasady działania sprawców. Odwoływali się oni do najprostszych technik inżynierii społecznej (*spear-phishing*), przesyłając wybranym użytkownikom zainfekowane wiadomości e-mail, po ich otworzeniu na twardym dysku instalowano złośliwe oprogramowanie, które pozwalało na skopiowanie jego zawartości. Najbardziej w ujawnionej kampanii uderzała jednak liczba zaatakowanych podmiotów, bo aż 71 należących tak do sektora publicznego, jak i prywatnego, w tym: 21 instytucji rządowych i międzynarodowych (6 na poziomie federalnym USA, 5 na poziomie stanowym, 3 na poziomie hrabstw, a także organy kanadyjskie, tajwańskie, wietnamskie, hinduskie oraz ONZ), 6 przedsiębiorstw przemysłu ciężkiego (budownictwo, hutnictwo), 13 przedsiębiorstw sektora IT oraz mediów (3 producentów urządzeń elektronicznych, 2 przed-

com/business/technology/china-hack-of-chamber-of-commerce-highlights-spear-phishing-dangers/2011/12/21/gIQAia709O_story.html; dostęp: 21.02.2014.

[309] E. Protalinski: *NASA: Hackers had 'full functional control'*. ZDNet, 02.03.2012: www.zdnet.com/blog/security/nasa-hackers-had-full-functional-control/10443; dostęp: 21.02.2014.

siębiorstwa produkujące programy antywirusowe, a także media informacyjne czy komunikacja satelitarna), 13 korporacji reprezentujących przemysł obronny, 6 instytucji i przedsiębiorstw sektora finansowego i rolniczego, a także 12 innych, w tym: 5 organizacji sportowych, 2 ośrodki badawcze czy polityczne organizacje *non-profit*. W sumie 49 z 71 zaatakowanych podmiotów pochodziło ze Stanów Zjednoczonych. Wśród nich znalazło się wiele komitetów olimpijskich i innych organizacji sportowych, które stały się ofiarami włamań w 2008 roku. Autorzy raportu powiązali je z Letnimi Igrzyskami Olimpijskimi, które rozpoczęły się w Pekinie w sierpniu. Warto dodać, iż sprawcy utrzymywali dostęp do zainfekowanych sieci średnio od miesiąca aż do 28 miesięcy (zob. Alperovitch, 2011). W raporcie, mającym bardzo ogólnikowy charakter, nie wskazano co prawda na odpowiedzialność kogokolwiek, jednak charakter zaprezentowanych danych, w tym przede wszystkim zaatakowane podmioty, ich lokalizacja geograficzna, sposób działania, a także zainteresowanie organizacjami sportowymi przed igrzyskami w Pekinie sugerowało wyraźnie zaangażowanie specjalistów z Chińskiej Republiki Ludowej. Wielu autorów i ekspertów mimo braku jednoznacznych dowodów właśnie w ten sposób interpretowało te informacje[310].

Wszystkie powyższe incydenty budziły w USA coraz większe obawy o możliwość wystąpienia cyberataków przeciwko infrastrukturze krytycznej. Świadczył o tym np. komunikat Departamentu Bezpieczeństwa Krajowego (DHS) z 2012 roku, w którym ujawniono czteromiesięczną kampanię teleinformatyczną wymierzoną w system gazociągowy Stanów Zjednoczonych. Stwierdzono w nim, że przy wykorzystaniu metod *spear-phishingu* (głównie podrobionych wiadomości e-mail) sprawcy podejmowali próby zdobycia nazw użytkownika i haseł komputerów niewielkiej grupy pracowników jednej z korporacji sektora energetycznego. Mimo różnych medialnych doniesień sugerujących sprawstwo Chin władze USA nie potwierdziły tej interpretacji. Incydent ten był jednak o tyle poważny, iż zagrażał instalacjom gazowym zabezpieczającym ok. 25% amerykańskiego zużycia energii[311]. W czerwcu 2012 roku doszło również do serii włamań wymierzonych w amerykański przemysł kosmiczny. Niedługo później dyrektor Agencji Bezpieczeństwa Narodowego (NSA) podał, że od 2009 roku liczba cyberataków wymierzonych w amerykańską infrastrukturę wzrosła aż 17-krotnie: z 9 do ok. 160[312]. Potwierdzeniem tych tendencji był ujawniony w grudniu 2012 roku incydent w dwóch amerykańskich elektrowniach.

[310] *China Suspected of Shady RAT Attacks*. „Information Week" 03.08.2011: www.informationweek.com/attacks/china-suspected-of-shady-rat-attacks/d/d-id/1099358; dostęp: 23.02.2014.

[311] *Gas Pipeline Cyber Intrusion Campaign*. „ICS-CERT Monthly Monitor", April 2012, s. 1; *Natural gas pipelines targeted by cyber attack*. ZDNet, 08.05.2012: www.infosecurity-magazine.com/view/25655/natural-gas-pipelines-targeted-by-cyber-attack; dostęp: 21.02.2014.

[312] J. Wolf: *Cyber Attacks Targeting U.S. Infrastructure Up 17-Fold Since 2009*. „The Huffington Post" 27.07.2012: www.huffingtonpost.com/2012/07/26/cyber-attacks-us-infrastructure_n_1708051.html; dostęp: 21.02.2014.

Jak stwierdzono w dokumencie ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), wykorzystano do tego złośliwe oprogramowanie, które przeniesiono do intranetu elektrowni za pomocą zainfekowanych pamięci USB. W jednym z dwóch przypadków był to wirus *Mariposa*. Niestety dokładne dane techniczne włamania nie zostały udostępnione opinii publicznej (*Malware infections*, 2012: 1—2).

Już na początku 2013 roku pojawiły się nowe doniesienia o cyberatakach z terytorium Chińskiej Republiki Ludowej. Tym razem zostały one wymierzone w najbardziej popularne amerykańskie media, w tym „The New York Times", „The Wall Street Journal", „The Washington Post", a także Bloomberg News. W przypadku pierwszej gazety włamania trwały w sumie cztery miesiące, a ich ofiarami padli m.in. dziennikarze pracujący w biurze w Szanghaju. Korporacja Mandiant, która badała te wydarzenia, stwierdziła jednoznacznie, iż stała za nimi Chińska Armia Ludowo-Wyzwoleńcza. W opinii niektórych mediów mogła to być zemsta za artykuł, w którym opisano fortunę zgromadzoną przez chińskiego premiera Wena Jiabao[313]. W przypadku „The Wall Street Journal" również włamano się do wewnętrznej sieci redakcji, gdzie poszukiwano informacji na temat najbliższych publikacji poświęconych Chinom[314]. W pozostałych dwóch przypadkach poza samym faktem cyberataku nie ujawniono żadnych dokładniejszych danych[315]. W lutym 2013 roku Departament Bezpieczeństwa Krajowego ujawnił kolejną kampanię cyberataków wymierzoną w amerykańską infrastrukturę krytyczną. W ciągu 6 miesięcy włamano się do 23 przedsiębiorstw sektora gazowego, wykorzystując do tego techniki inżynierii społecznej, w tym głównie podrobione wiadomości poczty elektronicznej zawierające złośliwe oprogramowanie. W ten sposób wykradziono wrażliwe dane dotyczące m.in. nazw użytkownika i haseł administratorów sieci, specyfiki ich działania, a także sposobów dostępu do systemów kontroli gazociągów. Potencjalnie mogły posłużyć do opracowania robaka o podobnych do *Stuxnetu* właściwościach. Mimo że w raporcie Departamentu Bezpieczeństwa Krajowego nie znalazło się bezpośrednie odniesienie do Chińskiej Republiki Ludowej, zdecydowana większość ekspertów wskazała właśnie na jej odpowiedzialność[316]. Równolegle w 2013 roku doszło do szeregu mniej istotnych incydentów teleinformatycznych. Jednym z nich było włamanie w maju na stronę Departamentu Pracy, na której zamieszczono złoś-

[313] *New York Times 'hit by hackers from China'*. BBC News, 31.01.2013: www.bbc.co.uk/news/world-asia-china-21271849; dostęp: 21.02.2014.

[314] *Wall Street Journal 'also a victim of China hacking attack'*. BBC News, 31.01.2013: www.bbc.co.uk/news/world-asia-china-21287757; dostęp: 21.02.2014.

[315] N. Perlroth: *Washington Post Joins List of News Media Hacked by the Chinese*. „The New York Times" 01.02.2013: www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html; dostęp: 21.02.2014.

[316] M. Clayton: *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*. „The Christian Science Monitor" 27.02.2013: www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage; dostęp: 21.02.2014.

liwe oprogramowanie przenoszące się automatycznie na twardy dysk każdego wizytującego ją użytkownika. Odpowiedzialnością za ten incydent obarczono osoby znajdujące się na terytorium ChRL[317]. W tym samym czasie wykryto również udaną penetrację sieci amerykańskiego korpusu wojsk inżynieryjnych (US Army Corps of Engineers), ponownie przeprowadzoną przez osoby zlokalizowane w Państwie Środka[318]. W październiku 2013 roku doszło do kolejnego chińskiego cyberataku wymierzonego tym razem w Federalną Komisję Wyborczą (Federal Election Commission). W jego wyniku zablokowano witrynę internetową tej instytucji[319].

Rok 2013 był przełomowy, jeśli chodzi o wykorzystanie cyberprzestrzeni w stosunkach amerykańsko-chińskich jeszcze z trzech powodów. Po pierwsze korporacja Mandiant od lat zajmująca się aktywnością ChRL w sieci opublikowała w lutym głośny raport na ten temat. Stwierdzono w nim, iż grupa dokonująca cyberataków na całym świecie określana mianem APT1 była *de facto* Drugim Biurem funkcjonującym w ramach III wydziału sztabu generalnego Chińskiej Armii Narodowo-Wyzwoleńczej. Zidentyfikowano go również jako „jednostkę nr 61398" zlokalizowaną w liczącym 130 000 metrów kwadratowych budynku przy ulicy Datong w Szanghaju. Na podstawie zaobserwowanej infrastruktury fizycznej uznano, iż pracują w niej setki lub nawet tysiące specjalistów zajmujących się prowadzeniem ofensywnych operacji w przestrzeni teleinformatycznej. Była ona wspierana m.in. przez China Telecom, która udostępniła na potrzeby jednostki specjalny światłowód. Mandiant ujawniło również, że od pracujących tam żołnierzy wymagano nie tylko wybitnych umiejętności informatycznych, lecz także świetnej znajomości języka angielskiego. W raporcie udostępniono również statystyki dotyczące sposobów działania jednostki nr 61398:

1. Od 2006 roku korporacja wykryła w sumie 141 udanych cyberataków na przedsiębiorstwa z 20 różnych gałęzi gospodarki.
2. Głównym obiektem jej zainteresowania była szeroko rozumiana własność intelektualna, w tym nowe technologie, schematy produkcyjne, rezultaty przeprowadzonych testów, opracowania dotyczące cen określonych produktów oraz porozumienia o partnerstwie.

---

[317] P. Ducklin: *US Department of Labor website hacked, serves malware, now fixed*. Sophos, 02.05.2013: http://nakedsecurity.sophos.com/2013/05/02/us-department-of-labor-website-hacked-serves-malware-now-fixed; dostęp: 21.02.2014; L. Bell: *US Department of Labor website hacked by a Chinese group*. „The Inquirer" 01.05.2013: www.theinquirer.net/inquirer/news/2265518/us-department-of-labor-website-hacked-by-a-chinese-group; dostęp: 21.02.2014.

[318] *US Army Corps of Engineers National Inventory of Dams hacked*. Security Affairs, 03.05.2013: http://securityaffairs.co/wordpress/14089/security/us-army-corps-engineers-national-inventory-of-dams-nid-hacked.html; dostęp: 21.02.2014.

[319] M. Henneberg: *Chinese hackers reportedly crashed Federal Election Commission website*. Fox News, 19.12.2013: www.foxnews.com/politics/2013/12/19/chinese-hackers-reportedly-crashed-federal-election-commission-website; dostęp: 21.02.2014.

3. Wykorzystywała nowatorskie techniki cyberataków, w tym dwa wcześniej niespotykane sposoby zdobywania poufnych wiadomości e-mail: GETMAIL oraz MAPIGET.
4. Średni okres dostępu do sieci i komputerów ofiar wynosił ok. 356 dni.
5. Ofiary APT1 pochodziły z reguły z tych sektorów gospodarki, które zostały przez Pekin uznane za strategiczne dla rozwoju ChRL.
6. Jednostka utrzymywała w ostatnich latach niemal tysiąc serwerów kontroli i dowodzenia (C&C), co świadczyło o ogromnej skali prowadzonych przez nią działań (*APT1*, 2012: 1—6).

Opublikowany raport stał się pierwszym opracowaniem w historii, które wyraźnie wyartykułowano i potwierdziło zdanie zdecydowanej większości ekspertów wskazujących od dawna na bezpośredni udział armii chińskiej w cyberatakach przeciwko Stanom Zjednoczonym. Udowodnił on, że ChRL od początku XXI wieku aktywnie rozwijała swoje zdolności nie tylko ukierunkowane na walkę zbrojną w sieci, ale także na szpiegostwo komputerowe. Omówione w dokumencie przypadki wyraźnie świadczyły też o tym, że większość wcześniejszych incydentów była w jakimś stopniu powiązana z Chinami, które w ten sposób chciały dogonić USA pod względem zdolności militarnych i technologicznych. Warto zauważyć, że opracowanie wywołało burzliwe reakcje rządu w Pekinie, który kategorycznie odrzucił jego wnioski[320].

W konsekwencji doprowadziło to do reakcji administracji Baracka Obamy, która po raz pierwszy na taką skalę dała do zrozumienia, że uznaje odpowiedzialność Chin za wrogie działania w cyberprzestrzeni. Znalazło to swój wyraz w raporcie Pentagonu opublikowanym w maju 2013 roku, w którym stwierdzono: „w 2012 [roku — M.L.] wiele systemów komputerowych na całym świecie, wliczając w to te należące do rządu USA, nadal były celem wtargnięć, z których część wydaje się bezpośrednio związana z rządem i wojskiem Chin" (*Annual Report to Congress*, 2013: 36). Zauważono tam, iż wykorzystują one aktywność

[320] Warto również pamiętać, iż część badaczy, jakkolwiek zgadzała się z tezą o udziale chińskich władz w działaniach cyberszpiegowskich wymierzonych w USA, stwierdziła, iż raport Mandiant nie dostarczył niepodważalnych dowodów w tej sprawie. W ten sposób argumentował m.in. Jeffrey Carr z Taia Global. Jednocześnie jednak należy mieć na uwadze, iż udowodnienie takiego sprawstwa w cyberprzestrzeni jest rzeczą niezwykle trudną. Raport Mandiant dostarczył natomiast sześciu grup argumentów, które jednoznacznie świadczyły o udziale jednostki wojskowej chińskiej armii. Dotyczyły one: zainteresowań sprawców, wykorzystywanych technik i procedur, skali dokonywanych operacji, specjalizacji personelu, lokalizacji geograficznej oraz wykorzystanej infrastruktury. Był więc jednym z bardzo nielicznych jawnych i niezależnych opracowań, które były w stanie z dużym prawdopodobieństwem wskazać na odpowiedzialność za cyberataki określonych struktur państwowych. Zob. M.J. Schwartz: *China Denies U.S. Hacking Accusations: 6 Facts*. Information Week, 21.02.2013: www.informationweek.com/attacks/china-denies-us-hacking-accusations-6-facts/d/d-id/1108750?page_number=2; dostęp: 21.02.2014; *APT1. Exposing One of China's Cyber Espionage Units*. Mandiant 2012, s. 59—60.

w cyberprzestrzeni do wsparcia swoich działań wywiadowczych wymierzonych w amerykańskie programy obronne. Według autorów zdobyte w ten sposób dane mogły być ponadto użyte do wsparcia chińskiego przemysłu (zarówno obronnego, jak i wysokich technologii), a także do przygotowania armii ChRL na ewentualny kryzys w stosunkach ze Stanami Zjednoczonymi (Ibidem, s. 36). Był to więc niezwykle doniosły dokument, w którym oskarżono chińskie władze o organizację wieloletnich operacji cyberszpiegowskich zagrażających amerykańskiemu bezpieczeństwu narodowemu.

W 2013 roku potwierdziły się opinie specjalistów, którzy od lat wskazywali, iż USA nie są w tym sporze jedynie stroną poszkodowaną, lecz również same dokonują cyberataków przeciwko Chinom. Zbiegły były pracownik amerykańskiej Agencji Bezpieczeństwa Narodowego Edward Snowden ujawnił dokumenty, według których w 2011 roku USA przeprowadziły w sumie 231 poważnych operacji w cyberprzestrzeni, których celem były Rosja, Chiny, Iran oraz Korea Północna. Cała kampania określona mianem GENIE miała kosztować ok. 652 mln dolarów. Zaangażowano w nią 1870 osób pracujących m.in. w kwaterze głównej NSA w Fort Meade[321]. Na tym tle warto przywołać komunikat chińskiego Ministerstwa Obrony, według którego w 2013 roku co miesiąc ChRL była atakowana w cyberprzestrzeni ok. 140 000 razy, a 63% z tych ataków pochodziło z terytorium Stanów Zjednoczonych (za: Grzelak, 2013: 118). Interesujące informacje ujawnił również Cai Minghzhao, minister Biura Informacyjnego Rady Państwa Chińskiej Republiki Ludowej, w trakcie swojego wystąpienia w Stanford University w listopadzie 2013 roku. Stwierdził wówczas, iż tylko między styczniem a sierpniem tego roku doszło do włamań na ponad 20 000 chińskich stron internetowych, a zagraniczni sprawcy przejęli kontrolę nad 8 mln komputerów, tworząc z nich sieć *botnet*. Stanowiło to wzrost o 14% w stosunku do poprzedniego roku[322]. Tym samym Pekin stał się w ostatnich latach częstą ofiarą cyberataków zagrażających jego bezpieczeństwu narodowemu. Potwierdzało to zarazem opinie wielu chińskich polityków, którzy wskazywali na daleko idącą hipokryzję Waszyngtonu w tej sprawie, ponieważ amerykańskie władze oraz media często akcentowały zagrożenie incydentami teleinformatycznymi sprokurowanymi przez ChRL, skrzętnie pomijano natomiast podobną działalność służb wywiadowczych USA[323].

[321] Geers, 2014: 5; B. Gellman, E. Nakashima: *U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show*. „The Washington Post" 31.08.2013: www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html; dostęp: 21.02.2014.

[322] C. Mingzhao: *Making Joint Efforts to Maintain Cyber Security*. China&US Focus. Engage. Stimulate. Impact, 21.11.2013: www.chinausfocus.com/peace-security/making-joint-efforts-to-maintain-cyber-security; dostęp: 23.02.2014.

[323] J. Davidson: *China Accuses U.S. of Hypocrisy on Cyberattacks*. „Time" 01.07.2013: http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks; dostęp: 21.02.2014.

Na tle omówionych wyżej przykładów można zaryzykować stwierdzenie, iż rywalizacja między Stanami Zjednoczonymi a Chińską Republiką Ludową w cyberprzestrzeni przybrała unikalną formę. Znane opinii publicznej przypadki incydentów teleinformatycznych miały charakter regularny oraz długotrwały, rozpoczęły się bowiem już pod koniec lat 90. XX wieku. Prawdopodobnie od początku pierwszej dekady XXI wieku w akcje wymierzone przeciwko instytucjom rządowym, badawczym oraz biznesowym USA włączyły się służby specjalne oraz wojsko Chińskiej Republiki Ludowej[324]. Organizowane przez nie operacje były na tyle poważne, iż zagroziły nawet amerykańskiej infrastrukturze krytycznej. Trudne do oszacowania są również straty, jakie poniesiono w wyniku kradzieży najnowszych technologii cywilnych i wojskowych. Równolegle cyberataki organizował także Waszyngton, co znacząco odbiegało od większości omówionych wcześniej przykładów. Nie dziwi więc fakt, iż zarówno politycy, jak i badacze coraz częściej zaczęli wskazywać, że incydenty te osiągnęły na tyle poważną skalę, aby determinować całokształt stosunków dwustronnych. Warto tutaj przytoczyć kilka z tych opinii. Ciekawe stanowisko zajął James A. Lewis (2010: 1), który w 2010 roku stwierdził, że w przypadku relacji amerykańsko-chińskich w cyberprzestrzeni, to, co było niegdyś rywalizacją ukrytą, zaczęło stawać się rywalizacją jawną. Ze strony chińskiej do źródeł tego stanu rzeczy zaliczył on chęć rozwoju asymetrycznych zdolności wojskowych, promocji rodzimych innowacji, a także odzyskania należnego miejsca w stosunkach międzynarodowych, ze strony amerykańskiej wskazał natomiast na dyskomfort związany z podatnością na ataki cyberszpiegowskie, erozję potęgi USA na arenie międzynarodowej oraz poczucie, że z globalnego systemu gospodarczego korzystają inne, wschodzące mocarstwa. Richard A. Clarke i Robert K. Knake (2010: 53, 62) zauważyli, iż cyberprzestrzeń mogłaby zostać potencjalnie wykorzystana przez Pekin do sparaliżowania amerykańskich grup lotniskowców wysłanych przykładowo do obrony Tajwanu. Tym samym byłby to czynnik odstraszający USA od zaangażowania w Azji Wschodniej. Ting Xu (2011) z Bertelsmann Foundation uznał, że dotychczasowe cyberataki występujące w stosunkach na linii Pekin — Waszyngton sprawiły, iż kwestia cyberwojny powinna stać się jednym z najistotniejszych elementów trwającego między nimi dialogu strategicznego. Zdaniem autora tylko takie rozwiązanie pozwoliłoby upewnić się, że dotychczasowa nieufność w tej dziedzinie nie przekształci się w działania wojenne. Według Anthony'ego H. Cordesmana oraz Justina G. Cordesmana (2001: 12) Pekin uczynił z walki w cyberprzestrzeni „krytyczną część swojej

[324] Warto podkreślić, iż był to jedynie pewien wycinek aktywności Chin w cyberprzestrzeni. Świadczyła o tym np. kampania cyberataków wymierzonych w ministerstwa spraw zagranicznych państw europejskich o kryptonimie *Ke3chang* w grudniu 2013 roku. Zob. *Operacja Ke3chang — chińscy hakerzy atakują europejską dyplomację*. Defence24.pl, 17.12.2013: www.defence24.pl/news_operacja-ke3chang-chinscy-hakerzy-atakuja-europejska-dyplomacje; dostęp: 7.04.2014.

doktryny wojskowej, częściowo po to, aby zniwelować przewagę, jaką Stany Zjednoczone posiadają w zakresie konwencjonalnych i atomowych zdolności do walki zbrojnej". Gen. Keith Alexander (2012) z Agencji Bezpieczeństwa Narodowego w kontekście ataków wymierzonych w amerykańskie korporacje zauważył, iż stanowią one „największy transfer bogactwa w historii". James C. Mulvenon (2013: 1) z Center for Intelligence Research and Analysis podkreślił, że cyberszpiegostwo jest najnowszą i „najbardziej dewastującą" formą chińskiej działalności wywiadowczej wymierzonej w amerykańską przewagę wojskową oraz technologiczną konkurencyjność. Tobias Feakin (2013: 8) z kolei uznał, iż aktywność cyberszpiegowska ChRL osiągnęła „skalę przemysłową". Richard Fisher (2011: 11) z International Assessment and Strategy Center określił natomiast ataki w cyberprzestrzeni mianem *cyberwojny*, szacując roczne straty z tego tytułu dla USA w granicach 200 mld dolarów. Można również wspomnieć słowa Magnusa Hjortdala (2011: 14), który zauważył, że włamania przeprowadzane przez Chiny są częścią ich strategii odstraszania Stanów Zjednoczonych przed rozpoczęciem konwencjonalnego konfliktu zbrojnego. Na tym tle wydaje się, iż natężenie cyberataków w stosunkach amerykańsko-chińskich przez ponad dekadę spełniło wymogi sformułowanej wcześniej definicji *cyberwojny*. Incydenty teleinformatyczne, mimo że w większości mające charakter *stricte* wywiadowczy, miały następujące cechy: zdarzały się regularnie, trwały od końca lat 90. XX wieku, miały charakter masowy, stwarzały poważne szkody finansowe, stwarzały zagrożenie dla bezpieczeństwa infrastruktury krytycznej, w znacznej części były przejawem zorganizowanych operacji prowadzonych przez służby obu państw, ich motywacją były przesłanki polityczne, gospodarcze lub wojskowe, wpisywały się w całokształt rywalizacji amerykańsko-chińskiej na arenie międzynarodowej oraz wywierały bezpośredni wpływ na charakter stosunków dwustronnych.

Mając na uwadze powyższe zagadnienia, należałoby wyodrębnić cele polityki zagranicznej, jakie realizowali obaj aktorzy, operując w cyberprzestrzeni. Ze strony chińskiej, jak wspomniano już wcześniej, można wyróżnić następujące przesłanki:

- wzmocnienie statusu ChRL jako mocarstwa na arenie międzynarodowej,
- wzmocnienie pozycji ChRL w stosunkach ze Stanami Zjednoczonymi,
- wyrównanie technologicznych i wojskowych dysproporcji względem USA,
- przyspieszenie rozwoju gospodarczego,
- zwiększenie efektywności działań wywiadowczych wobec USA,
- zbudowanie skutecznych asymetrycznych środków walki z US Army, a także osiągnięcie przewagi informacyjnej w przypadku ewentualnego konfliktu zbrojnego,
- odstraszanie Stanów Zjednoczonych od zaangażowania w Azji Wschodniej,
- odnalezienie oraz ewentualne wykorzystanie wrażliwych punktów w amerykańskiej infrastrukturze krytycznej w przypadku kryzysu w stosunkach bila-

teralnych (zob. Krekel, 2009: 10—22; Wortzel, 2013; Lai, Rahman, 2012; Wortzel, 2014; Bronk, 2011).

Warto przy tym pamiętać, że Chiny, działając w przestrzeni teleinformatycznej, nie atakowały wyłącznie Stanów Zjednoczonych, ale także ich sojuszników, zarówno w Azji, jak i w Europie. Można tu wymienić m.in. włamania do sieci brytyjskiego Ministerstwa Spraw Zagranicznych (Foreign Office) we wrześniu 2007 roku, południowokoreańskiego Ministerstwa Finansów w kwietniu 2009 roku, rządu Indii (m.in. biura doradcy ds. bezpieczeństwa narodowego) w styczniu 2010 roku, Ministerstwa Obrony Indii w kwietniu 2010 roku, marynarki wojennej Indii w lipcu 2012 roku, przedsiębiorstw EADS (European Aeronautic Defence and Space Company) i ThyssenKrupp w lutym 2013 roku czy australijskiego wywiadu ASIO (Australian Security Intelligence Organization) w maju 2013 roku[325].

Z drugiej strony znaczną aktywność w cyberprzestrzeni przeciwko ChRL wykazywały Stany Zjednoczone, w tym wypadku jednak ocena jej przesłanek jest o wiele trudniejsza, gdyż nie ma ogólnie dostępnych informacji na temat właściwości tych incydentów. Niemniej należy tu odnotować pewną ewolucję, która nastąpiła na szczytach władzy w Waszyngtonie. W *Strategy for Operating in Cyberspace* z 2011 zakładano przede wszystkim działania defensywne, nie przewidziano natomiast wojskowych operacji ofensywnych. W późniejszym czasie coraz więcej przedstawicieli US Army (w tym np. były dowódca sił amerykańskich w Afganistanie gen. Richard Mills) zaczęło jednak potwierdzać praktykę stosowania ataków komputerowych wobec wybranych, wrogich podmiotów[326]. O rozwoju szkodliwej aktywności w sieciach komputerowych świadczyło także powołanie omówionego już USCYBERCOM. Na tym tle można więc zaryzykować wyodrębnienie kilku najbardziej prawdopodobnych przesłanek amerykańskich cyberataków wobec ChRL. Należy do nich zaliczyć:

- powstrzymanie procesu wzmacniania chińskiej pozycji na arenie międzynarodowej,
- powstrzymanie chińskich prób zrównoważenia potencjałów technologicznych, militarnych i gospodarczych obu państw,
- cyberszpiegowstwo, mające charakter komplementarny w stosunku do standardowych technik wywiadowczych,
- utrzymanie przewagi informacyjnej nad ChRL, a także znalezienie skutecznych rozwiązań marginalizujących jej arsenał asymetrycznych środków walki,

---

[325] *Significant Cyber Incidents Since 2006*. Center for Strategic & International Studies, 30.01.2014: http://csis.org/files/publication/120806_Significant_Cyber_Incidents_Since_2006_0.pdf; dostęp: 17.02.2014.

[326] T. Gjelten: *First Strike: US Cyber Warriors Seize the Offensive*. „World Affairs Journal", January/February 2013: www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive; dostęp: 22.02.2014.

- podważenie legitymizacji Komunistycznej Partii Chin,
- odnalezienie wrażliwych punktów systemów i sieci kontrolujących chińską infrastrukturę krytyczną (Wortzel, 2013: 2).

Odwołując się do przywołanej wcześniej klasyfikacji celów polityki zagranicznej według Ryszarda Zięby, można więc stwierdzić, iż w obu przypadkach cyberprzestrzeń posłużyła jako nowy wymiar realizacji następujących założeń: zapewnienia bezpieczeństwa państwa, wzrostu jego siły oraz pozycji na arenie międzynarodowej.

Omówiona powyżej eskalacja rywalizacji w cyberprzestrzeni w ostatnich latach doprowadziła zarazem do pewnych modyfikacji polityki cyberbezpieczeństwa obu państw. Przejawem tych tendencji było przyjęcie przez administrację amerykańską w lutym 2013 roku *Administration Strategy to Mitigate the Theft of U.S. Trade Secrets*, w którym wyróżniono pięć grup założeń:

- zintensyfikowanie działań dyplomatycznych, w szczególności wobec krajów zaangażowanych w działalność cyberszpiegowską,
- wspieranie sektora prywatnego w celu wypracowania systemu dobrych praktyk,
- kontynuację działań Departamentu Sprawiedliwości na rzecz bardziej skutecznego wykrywania oraz karania kradzieży amerykańskich technologii przez zagranicznych rywali,
- kontynuację działań zmierzających do podnoszenia efektywności amerykańskiego prawa, jeśli chodzi o zwalczanie szpiegostwa przemysłowego,
- zwiększanie świadomości opinii publicznej co do zagrożenia kradzieżą amerykańskich tajemnic handlowych (*Administration Strategy*, 2013).

Na początku drugiej dekady XXI wieku doszło nawet do nawiązania ograniczonej współpracy rządów Chin i USA w zakresie zwalczania zagrożeń dla bezpieczeństwa teleinformatycznego, czym świadczyło kilka wydarzeń. Chęć podjęcia takich kroków wyraził nowy chiński premier Li Keqiang, twierdząc m.in., iż należy zakończyć „wojnę na słowa w sprawie cyberprzestrzeni" (cyt. za: Grzelak, 2013: 120). Wskazywały na to również kontakty przedstawicieli sztabów generalnych obu armii, którzy rozpoczęli rozmowy poświęcone kwestiom związanym z bezpieczeństwem teleinformatycznym. Wątek ten poruszono także w czerwcu 2013 roku podczas szczytu amerykańsko-chińskiego w Kalifornii. Wówczas Barack Obama zagroził, iż jeśli ataki ze strony chińskiej nie ustaną, będą się wiązały z poważnymi konsekwencjami w stosunkach gospodarczych obu państw (Grzelak, 2013: 120—121; *Cyber Detente*, 2012). W listopadzie 2013 roku, w trakcie wizyty w Stanach Zjednoczonych, minister Biura Informacyjnego Rady Państwa ChRL Cai Mingzhao przedstawił szereg propozycji w sprawie pogłębienia bilateralnej współpracy w dziedzinie cyberbezpieczeństwa. Przewidywały one m.in. poszanowanie narodowej suwerenności w cyberprzestrzeni, opracowanie systemu prawnego, który byłby w stanie skutecznie przeciwdziałać przejawom cyberprzestępczości oraz wzmocnienie współpracy

międzynarodowej, która powinna się oprzeć na trzech kwestiach: zdefiniowaniu podstawowych zasad zachowania państw w cyberprzestrzeni, wypracowaniu skutecznych sposobów przeciwdziałania wspólnym problemom w sieci, takim jak cyberterroryzm czy wirusy komputerowe, a także na stworzeniu nowych kanałów komunikacji, które powinny ułatwić międzynarodową kooperację w tej domenie[327].

W 2013 roku stworzono wspólną grupę roboczą ds. cyberbezpieczeństwa, którą wpisano w ramy strategicznego dialogu obu państw (*China — US Strategic Security Dialogue*). Zainaugurowała ona swoją działalność w lipcu, nie osiągnęła jednak w początkowym okresie żadnych konkretnych rezultatów[328]. Można zatem zaryzykować stwierdzenie, iż nawiązanie ograniczonej współpracy obu państw w tej dziedzinie nie oznaczało automatycznego przerwania poważnych cyberataków, jak wspomniano bowiem wyżej, rozmowom na wysokim szczeblu towarzyszyły kolejne poważne incydenty teleinformatyczne.

Reasumując ten wątek, należy podkreślić, iż cyberataki stały się jednym z najważniejszych problemów w stosunkach amerykańsko-chińskich od przełomu XX i XXI wieku. Szkodliwa działalność w przestrzeni teleinformatycznej wpisała się w narastającą rywalizację obu państw, przejawiającą się zarówno w płaszczyźnie politycznej, wojskowej, jak i gospodarczej. Na tym tle można więc zwrócić uwagę na kilka cech charakterystycznych tych problemów. Przede wszystkim należy podkreślić, iż cyberataki w stosunkach dwustronnych stanowiły rosnące zagrożenie dla bezpieczeństwa narodowego, przede wszystkim Stanów Zjednoczonych. Chińska armia oraz powiązane z nią grupy działały wielotorowo, odwołując się zarówno do najprostszych metod *phishingu*, jak i najbardziej zaawansowanych *exploitów* oraz złośliwych programów. Działania te miały charakter przede wszystkim wywiadowczy, obliczony na uzyskanie jak największej ilości wrażliwych informacji, które mogłyby być wykorzystane w rozgrywce z Waszyngtonem na innych obszarach rywalizacji. Poszukiwano nie tylko najnowszych technologii wojskowych czy informatycznych, ale także danych dotyczących specyfiki funkcjonowania infrastruktury krytycznej czy z pozoru nieistotnych materiałów dotyczących np. struktur organizacyjnych czy zastosowanych rozwiązań prawnych w poszczególnych przedsiębiorstwach. Co prawda nie doprowadziło to do bezpośrednich szkód fizycznych, tak jak miało to miejsce np. w Iranie, utrata tych informacji stanowiła jednak równie

[327] C. Mingzhao: *Making Joint Efforts to Maintain Cyber Security*. China&US Focus. Engage. Stimulate. Impact, 21.11.2013: www.chinausfocus.com/peace-security/making-joint-efforts-to-maintain-cyber-security; dostęp: 23.02.2014.

[328] *US — China cyber security working group meets*. BBC News, 09.07.2013: www.bbc.co.uk/news/world-asia-china-23177538; dostęp: 23.02.2014; *U.S., China agree to work together on cyber security*. Reuters, 13.04.2013: www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413; dostęp: 23.02.2014.

poważne zagrożenie dla amerykańskiej racji stanu. Po drugie wieloletnie operacje cyberszpiegowskie pozwoliły rzeczywiście zredukować technologiczną przepaść między ChRL oraz USA. Zdobycie przez Pekin wielu niezwykle drogich, najnowszych technologii pozwoliło na przyspieszenie rodzimych programów naukowo-technicznych. Świadczyły o tym np. liczne wypowiedzi przedstawicieli Pentagonu z 2013 roku, którzy wskazywali m.in. na związek utraty technologii z programu *Joint Strike Fighter* z szybkim rozwojem chińskich samolotów V generacji J-20 i J-31[329]. Na tej podstawie można więc stwierdzić, iż cyberprzestrzenne instrumenty polityki zagranicznej, przynajmniej w przypadku ChRL, okazały się w dużej mierze skuteczne. Zdanie to podzielało zresztą wielu amerykańskich badaczy i ekspertów. James Mulvenon stwierdził na przykład, iż „Chińczycy są pierwsi do używania cyberataków do [osiągania — M.L.] politycznych i wojskowych celów" (cyt. za: Lai, Rahman, 2012: 39). Po trzecie, jak wspomniano, natężenie incydentów teleinformatycznych w stosunkach dwustronnych osiągnęło w ostatnich latach taki poziom, iż można tutaj mówić o pojawieniu się zjawiska cyberwojny. Potwierdziły to zresztą badania niezależnych podmiotów, takich jak np. Mandiant, a także informacje i dokumenty ujawnione przez Edwarda Snowdena, choć, jak stwierdził Larry M. Wortzel, bez względu na to Chińska Republika Ludowa będzie temu oficjalnie zaprzeczać (Wortzel, 2013: 2). Niemniej kwestia odpowiedzialności obu rządów za operacje w cyberprzestrzeni wydaje się przesądzona. Jest to tym bardziej ewidentne, iż sprawcy najpoważniejszych cyberataków nie ponieśli odpowiedzialności za swoje czyny.

Na tym tle można więc stwierdzić, iż cyberprzestrzeń stała się kolejnym wymiarem rywalizacji, a czasami wręcz konfrontacji między Chińską Republiką Ludową a Stanami Zjednoczonymi. *Casus* ten był o tyle wyjątkowy, iż ataki komputerowe miały wpływ na relacje bilateralne już od końca lat 90. XX wieku. Przez lata czyniły coraz poważniejsze szkody, a dopiero w 2013 roku zainspirowały pierwsze kroki, których celem było nawiązanie dwustronnej współpracy w tej dziedzinie, choć jej dotychczasowa skuteczność okazała się niewielka.

[329] *Theft of F-35 design data is helping U.S. adversaries — Pentagon*. Reuters, 19.06. 2013: www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619; dostęp: 23.02.2014.

Rozdział 5

Cyberprzestrzeń jako nowy wymiar współpracy państw

Wszystkie omówione w poprzednim rozdziale przykłady rywalizacji państw w cyberprzestrzeni pozwalają stwierdzić, że różnorodnie motywowane cyberataki bez wątpienia stanowią narastające zagrożenie nie tylko dla ich bezpieczeństwa, lecz także całej wspólnoty międzynarodowej. Godząc bezpośrednio lub pośrednio w interesy rządów, przekładają się one na stosunki polityczne między nimi, mogą zatem prowadzić do destabilizacji sytuacji międzynarodowej. Sytuację pogarsza rosnące uzależnienie od ICT oraz coraz większa aktywność podmiotów pozapaństwowych online. Jak wskazano wcześniej, wyzwania dla bezpieczeństwa teleinformatycznego mają tylko częściowo związek z działalnością poszczególnych krajów. Resztę stanowią hakerzy, haktywiści, terroryści czy przestępcy. Przeciwdziałanie tym wyzwaniom jedynie na poziomie narodowym jest niezwykle trudne, zarówno ze względu na globalny charakter infrastruktury teleinformatycznej, jak i „ageograficzność" Internetu.

Na tym tle od przełomu XX i XXI wieku można jednak dostrzec pewną interesującą tendencję w środowisku międzynarodowym. Otóż poszczególne podmioty, rywalizując czy wręcz konfrontując się w cyberprzestrzeni, są zarazem coraz bardziej zainteresowane rozwojem współpracy w tym wymiarze. Regulacja przestrzeni teleinformatycznej, która, jak wiadomo, posiada szereg unikalnych właściwości, jest zadaniem niezwykle trudnym, lecz niezbędnym, aby uniknąć dalszej proliferacji tego typu działań, mogących doprowadzić do trudnych do przewidzenia konsekwencji dla bezpieczeństwa narodowego i międzynarodowego, szczególnie jeśli zachowane zostanie dotychczasowe tempo procesów komputeryzacji i informatyzacji. Warto szerzej omówić najbardziej interesujące inicjatywy w tej dziedzinie oraz ich efektywność w zwalczaniu najpoważniejszych cyberzagrożeń.

5.1. Organizacja Narodów Zjednoczonych wobec wyzwań dla bezpieczeństwa teleinformatycznego[1]

Jedną z pierwszych i najważniejszych organizacji międzynarodowych, które zainteresowały się tematyką cyberbezpieczeństwa, była z pewnością Organizacja Narodów Zjednoczonych. Jako struktura uniwersalna, skupiająca zdecydowaną większość państw świata, od początku miała do odegrania fundamentalną rolę w tej dziedzinie. Wynikało to przede wszystkim z zapisów *Karty Narodów Zjednoczonych*, które narzuciły jej obowiązki czuwania nad pokojem i bezpieczeństwem międzynarodowym. W artykule 1. KNZ stwierdzono, iż obowiązkiem ONZ jest:

> Utrzymać międzynarodowy pokój i bezpieczeństwo, stosując skuteczne środki zbiorowe dla zapobiegania zagrożeniom pokoju i ich usuwania, tłumienia aktów agresji i innych naruszeń pokoju, łagodzić i załatwiać — w drodze pokojowej, według zasad sprawiedliwości i prawa międzynarodowego — spory lub sytuacje mogące prowadzić do naruszenia pokoju.

W artykule 2. uznano, że

> Wszyscy członkowie załatwiać będą swe spory międzynarodowe środkami pokojowymi w taki sposób, aby nie dopuścić do zagrożenia międzynarodowego pokoju i bezpieczeństwa oraz sprawiedliwości […]. Wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od stosowania groźby lub użycia siły przeciwko całości terytorialnej lub niepodległości któregokolwiek państwa.

Istotne znaczenie zyskał tu również artykuł 51, w który stwierdza się:

> Żadne postanowienie niniejszej Karty nie narusza naturalnego prawa każdego członka Organizacji Narodów Zjednoczonych, przeciwko któremu dokonano zbrojnej napaści, do indywidualnej lub zbiorowej samoobrony, zanim Rada Bezpieczeństwa zastosuje środki, konieczne dla utrzymania międzynarodowego pokoju i bezpieczeństwa[2].

Zapisy tych trzech artykułów zyskały fundamentalne znaczenie dla całokształtu stosunków międzynarodowych po drugiej wojnie światowej. Ich specyfika naturalnie nadawała ONZ podstawowe kompetencje do zwalcza-

[1] Rozdział został opracowany na podstawie artykułu: Lakomy, 2013a.

[2] *Karta Narodów Zjednoczonych*. Ośrodek Informacji Organizacji Narodów Zjednoczonych, Warszawa: www.unic.un.org.pl/dokumenty/karta_onz.php; dostęp: 24.02.2014.

nia nowych zagrożeń dla bezpieczeństwa międzynarodowego, również tych związanych z powstaniem i rozwojem cyberprzestrzeni. Stało się to tym bardziej ewidentne, iż z czasem pojawiło się omówione wyżej zjawisko rywalizacji państw w tej nowej, dotychczas nie poddanej wystarczającym regulacjom domenie. Można zaryzykować stwierdzenie, że to w gruncie rzeczy ten problem stał się kluczowy dla organizacji, której głównym zadaniem powinno być wypracowywanie nowych politycznych i prawnych mechanizmów kooperacji lub współistnienia wszystkich podmiotów międzynarodowych w cyberprzestrzeni.

Zainteresowanie Organizacji Narodów Zjednoczonych oraz jej organizacji wyspecjalizowanych tematyką cyberbezpieczeństwa rozpoczęło się stosunkowo wcześnie, bo już w latach 80. XX wieku. W połowie dekady na Siódmym Kongresie Narodów Zjednoczonych w Sprawie Zapobiegania Przestępczości i Postępowania ze Sprawcami (Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders) zauważono możliwość występowania nowych typów przestępczości zorganizowanej, związanych z wykorzystaniem technologii komputerowych. W związku z tym wezwano społeczność międzynarodową do nawiązania współpracy, która pozwoliłaby zapobiec pojawianiu się nowych wyzwań m.in. dla podstawowych praw człowieka, w tym prawa do prywatności (*Seventh United Nations Congress*, 1985: 14). Już w rok później Rada Gospodarcza i Społeczna ONZ zwróciła uwagę na ten problem w rezolucji nr 12/1986. Podkreślono w niej znaczenie systemów informatycznych jako istotnych środków zwalczania przestępczości (*Crime prevention*, 1986). W grudniu 1989 roku sprawą zajęło się także Zgromadzenie Ogólne ONZ, które w rezolucji nr 44/72 dostrzegło przydatność nowych technologii do łamania prawa (*Crime Prevention*, 1989).

Nieco szerzej problem ten został poruszony dopiero w roku 1990, w trakcie Ósmego Kongresu Narodów Zjednoczonych w Sprawie Zapobiegania Przestępczości i Postępowania ze Sprawcami (Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders), który odbył się w Hawanie. Zwrócono wówczas większą niż dotychczas uwagę na pojawienie się nowego fenomenu, jakim była przestępczość komputerowa. Uczestnicy Kongresu uznali, iż najnowsze technologie oraz zaawansowana wiedza techniczna mogą służyć za dogodne instrumenty działalności przestępczej. Jako przykład podano tu m.in. oszustwa komputerowe. W raporcie końcowym znalazła się zatem rekomendacja dotycząca nawiązania współpracy między wybranymi agencjami państwowymi w celu skutecznego zwalczania nowych zagrożeń. Podkreślono również znaczenie ICT jako skutecznego środka zwalczania aktów kryminalnych (*Eight United Nations Congress*, 1990: 11—14).

Mimo tych zapisów w pierwszej połowie lat 90. XX wieku Organizacja Narodów Zjednoczonych w swoich pracach raczej sporadycznie odnosiła się do wyzwań dla bezpieczeństwa teleinformatycznego, traktując te zagadnienia

raczej jako pewną ciekawostkę niż rzeczywisty problem. Kwestie te poruszono np. na Dziewiątym Kongresie Narodów Zjednoczonych w Sprawie Zapobiegania Przestępczości i Postępowania ze Sprawcami (Nineth United Nations Congress on the Prevention of Crime and the Treatment of Offenders) zorganizowanym w Kairze (*Ninth United Nations Congress*, 1995). Sprawą zainteresowała się także Konferencja Narodów Zjednoczonych ds. Handlu i Rozwoju, która na 9. sesji w Midrandzie zauważyła rosnące znaczenie technologii ICT (*Adoption of the agenda*, 1996). Można również wspomnieć o opublikowanym w 1994 roku poradniku na temat zapobiegania i kontroli społecznej cyberprzestępczości: *International review of criminal policy — United Nations Manual on the prevention and control of computer-related crime* (Siwicki, 2013: 29). Poza tymi krótkimi wzmiankami nie podjęto jednak wówczas żadnych wiążących decyzji, które przyczyniłyby się do pojawienia się skutecznych mechanizmów kooperacji między rządami.

Do pewnej zmiany w tym zakresie doszło dopiero pod koniec lat 90. XX wieku. Wiązało się to z jednej strony z coraz widoczniejszymi negatywnymi konsekwencjami rewolucji informatycznej, z drugiej natomiast władze wielu państw, w tym m.in. Rosji czy USA, zainteresowały się po raz pierwszy na szerszą skalę rozwojem współpracy międzynarodowej w tej dziedzinie (zob. Maurer, 2011: 5). W efekcie na 53. sesji Zgromadzenia Ogólnego ONZ w styczniu 1999 roku uchwalono rezolucję nr 53/70 zatytułowaną *Rozwój w obszarze informacji i telekomunikacji w kontekście międzynarodowego bezpieczeństwa*. Zawarto w niej wiele istotnych spostrzeżeń. Przede wszystkim stwierdzono, iż proliferacja technologii informacyjnych może zostać wykorzystana przeciwko stabilności i bezpieczeństwu całej społeczności międzynarodowej, a także poszczególnych państw członkowskich ONZ. W związku z tym wezwano je do podjęcia wielostronnej współpracy, której celem byłoby zidentyfikowanie istniejących oraz potencjalnych zagrożeń w tej dziedzinie. Ponadto zwrócono się do nich o przesłanie sekretarzowi generalnemu swoich opinii i ocen dotyczących m.in. ogólnego spojrzenia na kwestie bezpieczeństwa informacyjnego, sposobów zdefiniowania głównych kategorii i pojęć w tym zakresie, a także możliwości wykształcenia międzynarodowych zasad, które pozwoliłyby efektywniej zwalczać „informacyjny terroryzm i przestępczość" (*Resolution 53/70*, 1999). Należy podkreślić, iż był to pierwszy tego typu dokument ZO ONZ, w którym nie tylko zwrócono uwagę na narastające zagrożenia cyberbezpieczeństwa, ale także wskazano na pewne podstawowe sposoby przeciwdziałania im.

Choć sama rezolucja nie skutkowała żadnymi poważnymi przedsięwzięciami, to przyczyniła się do tego, iż na wiele lat Zgromadzenie Ogólne ONZ stało się głównym organem zajmującym się tą problematyką. Wyrazem tego było położenie większego nacisku na te zagadnienia podczas jego 54. sesji. Pierwszy Komitet do swojej agendy prac zaliczył właśnie kwestie związane z wpływem rozwoju najnowszych technologii na bezpieczeństwo międzynarodowe (*Docu-*

ments of the First Committee, 1999). Efektem większego niż dotychczas zaangażowania społeczności międzynarodowej w debatę na temat bezpieczeństwa teleinformatycznego stało się kilka rezolucji. W pierwszej, nr 54/49, Zgromadzenie Ogólne, odnotowując rozwój technologii informacyjnych oraz telekomunikacji, a także ich znaczenie dla współczesnych państw, zauważyło, iż mogą one mieć zastosowanie nie tylko cywilne, ale i wojskowe. W związku z tym powtórzono wcześniejsze wezwania do nawiązania bliższej współpracy rządów w tej dziedzinie oraz do kontaktów z sekretarzem generalnym ONZ (*Resolution 54*/*49*, 1999). Do tych zagadnień pośrednio odwołała się również rezolucja nr 54/50, w której zaapelowano do krajów członkowskich m.in. o określenie jasnych zasad transferu najnowszych technologii cywilnych i wojskowych w taki sposób, aby nie zagrażało to bezpieczeństwu międzynarodowemu (*Resolution 54*/*50*, 1999). Warto także wspomnieć o rezolucji nr 54/201, która skupiła się przede wszystkim na promocji współpracy państw oraz sektora prywatnego w zakresie najnowszych rozwiązań naukowo-technicznych (*Resolution 54*/*201*, 2000).

Za szczególnie istotną na tym etapie prac należy jednak uznać rezolucję nr 55/63, w której podkreślono potrzebę nawiązania kooperacji państw członkowskich w walce z przestępczością komputerową. Stwierdzono tam ponadto, iż poszczególne rządy powinny zaktualizować swoje systemy prawne w taki sposób, aby nie stawać się „bezpieczną przystanią" dla cyberprzestępczości. Zauważono także, że walka z nią powinna wziąć pod uwagę również kwestię ochrony podstawowych praw człowieka (*Resolution 55*/*63*, 2001). Warto wspomnieć również o *Deklaracji Milenijnej Narodów Zjednoczonych*, w której uznano, iż „korzyści, jakie dają nowe technologie, a w szczególności technologie informacyjne i komunikacyjne", powinny stać się „dostępne dla wszystkich ludzi" (*Deklaracja Milenijna*, 2002: 7). Na tej podstawie można więc zauważyć, iż Organizacja Narodów Zjednoczonych skupiła się na przełomie wieków na dwóch grupach problemów. Z jednej strony starano się inicjować współpracę zmierzającą do zwalczania cyberprzestępczości, z drugiej natomiast dostrzeżono również ewentualne negatywne polityczne i wojskowe konsekwencje szkodliwej działalności w przestrzeni teleinformatycznej.

W kolejnych latach tego typu optyka została przez Zgromadzenie Ogólne ONZ podtrzymana. Świadczyła o tym przede wszystkim rezolucja nr 56/121, w której ponownie skupiono się na walce z nielegalnym wykorzystaniem technologii informacyjnych, podkreślając dotychczasowy dorobek Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości (Commission on Crime Prevention and Criminal Justice). Wezwano również państwa członkowskie do korzystania z niego w pracach nad narodowymi strategiami zwalczania cyberprzestępczości (*Resolution 56*/*121*, 2002). Po drugie w 2002 roku przy współpracy m.in. Stanów Zjednoczonych, Federacji Rosyjskiej, Francji oraz Korei Południowej (Maurer, 2011: 43) uchwalono rezolucję nr 57/239, która

została poświęcona budowie „globalnej kultury cyberbezpieczeństwa". Zauważając rosnące uzależnienie krajów członkowskich (w tym ich sektora prywatnego) od prawidłowego funkcjonowania technologii informacyjnych, wezwano społeczność międzynarodową do jej współtworzenia. Miała ona zostać oparta na 9 elementach:

- świadomości potrzeby zapewnienia bezpieczeństwa systemów i sieci informacyjnych,
- odpowiedzialności za bezpieczeństwo systemów informacyjnych we właściwym do pełnionych ról zakresie,
- prewencji, wykrywaniu i odpowiadaniu na incydenty teleinformatyczne, m.in. poprzez wymianę informacji na temat głównych zagrożeń,
- etyce polegającej na poszanowaniu interesów innych podmiotów korzystających z systemów i sieci informacyjnych,
- uwzględnieniu wartości demokratycznych,
- prowadzeniu regularnych ocen ryzyka,
- uwzględnieniu wymogów bezpieczeństwa w projektach i planach wykorzystania sieci i systemów informacyjnych,
- dynamicznym zarządzaniu bezpieczeństwem,
- ponownej ocenie przyjętych już rozwiązań w tym zakresie (*Resolution 57/239*, 2003).

Była to jedna z najciekawszych ówczesnych inicjatyw podjętych przez organy ONZ, stanowiła bowiem wyraz zrozumienia, że ze względu na globalny charakter wyzwań teleinformatycznych również odpowiedź powinna mieć charakter ogólnoświatowy. Świadczyła ona również, że wśród elit politycznych rośnie świadomość narastających zagrożeń w cyberprzestrzeni. Potwierdzeniem tego kierunku działania stała się rezolucja nr 58/199 z grudnia 2003 roku poświęcona dalszej budowie globalnej kultury cyberbezpieczeństwa oraz ochronie krytycznej infrastruktury informacyjnej. Zwrócono tam m.in. uwagę na potrzebę zasypania „cyfrowych podziałów" na świecie poprzez promocję powszechnego dostępu do technologii ICT. Szczególny nacisk w dokumencie położono jednak przede wszystkim na ustalenie podstawowych sposobów ochrony infrastruktury krytycznej. Zaproponowano następujące rozwiązania:

- stworzenie sieci ostrzegania o zagrożeniach i incydentach teleinformatycznych,
- podnoszenie świadomości i zrozumienia interesariuszy (*stakeholders*) na temat funkcjonowania infrastruktury krytycznej i potrzeb jej ochrony,
- badanie infrastruktury krytycznej i identyfikacja współzależności między jej poszczególnymi elementami,
- promocja partnerstwa między interesariuszami,
- stworzenie i utrzymanie kryzysowych sieci komunikacyjnych,
- zapewnienie, aby polityki dostępności danych brały pod uwagę potrzeby ochrony informacyjnej infrastruktury krytycznej,

- zapewnienie możliwości śledzenia ataków na informacyjną infrastrukturę krytyczną oraz ujawnianie w wybranych przypadkach tego typu danych innym państwom,
- prowadzenie ćwiczeń i szkoleń z zakresu cyberbezpieczeństwa,
- posiadanie odpowiedniego systemu prawnego oraz wyszkolonego personelu, co umożliwi prowadzenie dochodzeń oraz karanie sprawców ataków na informacyjną infrastrukturę krytyczną,
- zaangażowanie we współpracę międzynarodową w tej dziedzinie, która miałaby polegać m.in. na koordynacji dochodzeń oraz wymianie informacji o zagrożeniach teleinformatycznych,
- promocja prac badawczo-rozwojowych, zarówno na poziomie narodowym, jak i międzynarodowym (*Resolution 58*/*199*, 2004).

Była to zatem kolejna istotna rezolucja Zgromadzenia Ogólnego Narodów Zjednoczonych, która podjęła jeden z kluczowych problemów dla cyberbezpieczeństwa całej społeczności międzynarodowej. Zaproponowane działania, jakkolwiek sformułowane dość ogólnikowo, mogły jednak stanowić podstawę do dalszych, bardziej skonkretyzowanych inicjatyw globalnych w tym zakresie.

W połowie pierwszej dekady XXI wieku Zgromadzenie Ogólne zaczęło jednak nieco mniej interesować się tą problematyką, redukując swoje znaczenie raczej do roli gremium wspierającego przedsięwzięcia innych organów ONZ. Świadczyły o tym kolejne rezolucje, które przestały wnosić nowe i ciekawe wątki do debaty poświęconej bezpieczeństwu teleinformatycznemu. W rezolucji nr 60/45 z 8 grudnia 2005 roku np. po prostu powtórzono apel, aby państwa członkowskie rozwijały współpracę w zakresie bezpieczeństwa informacyjnego (*Resolution 60*/*45*, 2006). Nieco później, mimo wydarzeń z Estonii i Gruzji, które wzmogły zainteresowanie innych organizacji międzynarodowych tymi zagadnieniami, Zgromadzenie Ogólne nie wykazało zwiększonej aktywności. W kolejnych rezolucjach powielano jedynie wezwania do pogłębionej kooperacji państw. W ten sposób sformułowano m.in. dokumenty o sygnaturach 61/54, 62/17, 63/37, 64/25 czy 66/24 (*Resolution 61*/*54*, 2006; *Resolution 62*/*17*, 2008; *Resolution 63*/*37*, 2009; *Resolution 64*/*25*, 2010; *Resolution 66*/*24*, 2011). Co prawda przyjmowano i inne rezolucje dotyczące szeroko pojętego rozwoju technologicznego (np. nr 62/182 z 19 grudnia 2007 roku), jednak *de facto* nie miały one większego znaczenia politycznego. Jedynym w zasadzie wyjątkiem, który odbiegał od tych niewiele znaczących inicjatyw, był dokument nr 64/211 ponownie poświęcony budowie globalnej kultury cyberbezpieczeństwa oraz ochronie infrastruktury krytycznej. Poszerzono w nim i uszczegółowiono listę priorytetowych działań, które powinny podjąć rządy w tej dziedzinie (*Resolution 64*/*211*, 2010). Na tym tle należy więc zauważyć, iż rola Zgromadzenia Ogólnego ONZ jako organu podejmującego próby inicjowania międzynarodowej współpracy w zakresie bezpieczeństwa teleinformatycznego zaczęła w drugiej połowie pierwszej dekady XXI wieku maleć.

Obowiązki dotyczące rozwoju polityki cyberbezpieczeństwa w coraz większym stopniu przejmowały jednak inne struktury funkcjonujące w ONZ. Jedną z nich był sekretarz generalny, który od początku okresu pozimnowojennego przejawiał rosnące zainteresowanie tą sferą. Wśród najważniejszych, pełnionych przez niego funkcji można wymienić:

- zbieranie sugestii i opinii państw członkowskich co do sposobów zwalczania zagrożeń teleinformatycznych,
- informowanie ich o wnioskach z zebranych sugestii i opinii,
- promowanie międzynarodowej debaty na temat cyberbezpieczeństwa, czego wyrazem były m.in. spotkania ekspertów w sierpniu 1999 roku oraz kwietniu 2008 roku, zorganizowane wraz z Instytutem Narodów Zjednoczonych ds. Badań nad Rozbrojeniem (United Nations Institute for Disarmament Research),
- promowanie praktycznej współpracy państw m.in. poprzez powołaną w 2005 roku Antyterrorystyczną Zadaniową Grupę Realizacyjną (Counter-Terrorism Implementation Task Force),
- wspieranie badań nad cyberbezpieczeństwem za pomocą zespołów ekspertów rządowych,
- wykonywanie innych zaleceń Zgromadzenia Ogólnego ONZ[3].

Oprócz sekretarza generalnego warto zwrócić uwagę jeszcze na dwie struktury. Pierwszą jest naturalnie Rada Bezpieczeństwa, która zgodnie z zapisami Karty NZ ma obowiązek czuwania nad międzynarodowym pokojem i bezpieczeństwem (Bierzanek, Symonides, 2002: 308). W okresie pozimnowojennym organ ten wykazywał marginalne zainteresowanie tą problematyką. Wszyscy stali członkowie Rady Bezpieczeństwa mimo dynamicznego rozwijania przez siebie ofensywnych i defensywnych zdolności do działania w cyberprzestrzeni przez lata nie przejawiali większych ambicji do użycia RB ONZ jako platformy zwalczania podstawowych zagrożeń teleinformatycznych. Co prawda niektóre z rezolucji Rady, w tym np. nr 1368 z 12 września 2001 roku oraz nr 1373 z 28 września 2001 roku, mogłyby być potencjalnie odniesione również do poważnych cyberataków, taka ich szeroka interpretacja budziłaby jednak zapewne kontrowersje (Melzer, 2011: 2). Należy więc podkreślić, iż Rada Bezpieczeństwa nie odniosła się w żaden sposób do coraz poważniejszych incydentów teleinformatycznych. Mimo groźnych wydarzeń w Estonii, Gruzji czy Korei Południowej stali członkowie Rady w żadnej z uchwalonych przez siebie rezolucji nie ustosunkowali się do tych problemów. Wydaje się, że ten stan rzeczy wynikał z dwóch powodów. Po pierwsze, jak wykazano w poprzednim rozdziale, większość stałych członków Rady Bezpieczeństwa ONZ lub ich sojuszników

[3] Zob. np. *Resolution 68/243*, 2014, s. 3; *The United Nations Global Counter-Terrorism Strategy*, 2006; *Counter-Terrorism Implementation Task Force*. United Nations: www.un.org/en/terrorism/ctitf/index.shtml; dostęp: 14.01.2012.

było zaangażowanych w takiej lub innej formie w rozmaite ofensywne operacje w cyberprzestrzeni od początku XXI wieku. W związku z tym nie było podstaw do osiągnięcia konsensusu, kiedy w wielu przypadkach Stany Zjednoczone, Rosja lub Chiny nie były zainteresowane zwróceniem uwagi na dane incydenty. Po drugie natomiast wiązało się to z zupełnie odmiennymi priorytetami w sprawie pożądanych form współpracy międzynarodowej w wymiarze cyberbezpieczeństwa, jakie formułowano w Waszyngtonie, Moskwie czy Pekinie.

Z jednej strony, co dość znamienne, w pierwszej dekadzie XXI wieku jednymi z największych zwolenników uregulowania zagadnień związanych ze zjawiskiem cyberwojny były Federacja Rosyjska oraz Chińska Republika Ludowa. Jak zauważył Pasha Sharikov (2013: 3—4). Moskwa była zainteresowana przyjęciem międzynarodowego dokumentu, który uregulowałby podstawowe wątpliwości związane z cyberbezpieczeństwem w oparciu o takie normy, jak zasada nieinterwencji w sprawy wewnętrzne, zakaz użycia siły, poszanowanie praw człowieka i zakaz wykorzystania ICT w sposób niezgodny z Kartą Narodów Zjednoczonych. Zbliżoną politykę prowadził Pekin, który również podkreślał potrzebę uregulowania podstawowych kwestii związanych z działaniami w cyberprzestrzeni w oparciu o porozumienia dwu- i wielostronne. Co więcej, ChRL popierała pomysł przekazania nadzoru nad tymi zagadnieniami wybranej instytucji ponadnarodowej. Michael D. Swaine wskazał na trzy najważniejsze cele chińskiej polityki cyberbezpieczeństwa na arenie międzynarodowej:

- postrzeganie zagrożeń teleinformatycznych jako problemu globalnego,
- uznanie cyberataków za wyzwanie dla narodowej suwerenności, porządku wewnętrznego i stabilności społecznej,
- wspieranie międzynarodowych wysiłków na rzecz opracowania podstawowych norm, reguł i zasad wspierających nadzór poszczególnych państw nad narodową cyberprzestrzenią.

Zdaniem Swaine'a Chiny krytycznie podchodziły do polityki państw zachodnich, w tym głównie Stanów Zjednoczonych, oskarżając je o postępującą militaryzację cyberprzestrzeni, stosowanie podwójnych standardów, jeśli chodzi o zapewnianie sobie „cyberwolności" przy jednoczesnym ograniczaniu jej innym, formułowanie bezpodstawnych oskarżeń wobec Pekinu, a także dominowanie we współczesnym „cybersystemie"[4]. W tym kontekście oba państwa wspierane m.in. przez Szanghajską Organizację Współpracy od lat wskazują więc na potrzebę globalnego uregulowania podstawowych zagadnień związanych z cyberbezpieczeństwem. Świadczyła o tym najdobitniej znamienna reakcja chińskich władz w lutym 2013 roku na omówiony już raport korporacji Mandiant. Gdy oskarżono w nim Chińską Armię Ludowo-Wyzwoleńczą

[4] M.D. Swaine: *Chinese Views on Cybersecurity in Foreign Relations*. Carnegie Endowment, s. 1, 13—15: http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf; dostęp: 26.02.2014.

o organizację cyberataków wymierzonych w USA, przedstawiciel Ministerstwa Obrony Narodowej Geng Yansheng stwierdził, iż nie ma powszechnie przyjętej przez społeczność międzynarodową definicji tego, czym jest *de facto* „atak hakerski”[5]. Warto zauważyć, iż stanowiska rosyjskie i chińskie w tej sprawie posiadają jeszcze jedną cechę wspólną, ponieważ w obu przypadkach akcentuje się zasadnicze znaczenie cyberprzestrzeni jako nowej domeny działań propagandowych. Już w 2008 roku podczas konferencji rozbrojeniowej ONZ rosyjski minister obrony podkreślił, iż jeśli jakiś rząd promowałby wolność słowa w sieci lub hasła demokratyzacji z zamiarem obalenia legalnych władz, Moskwa zinterpretowałaby takie działania jako agresję i ingerencję w jej sprawy wewnętrzne. Taka optyka wynika ze świadomości, iż protesty społeczne mogą być generowane także za pomocą akcji prowadzonych głównie w Internecie. Jest to tym bardziej ewidentne, iż w opinii Rosjan mogą być one inspirowane lub finansowane przez obce służby specjalne (Giles, 2012: 71—74). W tej sytuacji Federacja Rosyjska oraz Chińska Republika Ludowa odnoszą się niechętnie do inicjatyw, które ograniczyłyby ich kontrolę nad narodową cyberprzestrzenią. Wyrazem tego typu tendencji była rosyjska odmowa podpisania *Konwencji Rady Europy o cyberprzestępczości*[6]. W zamian na początku drugiej dekady XXI wieku Rosja zaproponowała rozpoczęcie prac nad nową globalną umową w tej sprawie, uznając porozumienie z 2001 roku za zdezaktualizowane[7].

Symbolicznym przejawem zaangażowania tandemu rosyjsko-chińskiego w rozwój międzynarodowej współpracy w dziedzinie cyberbezpieczeństwa stał się jednak przede wszystkim list skierowany do sekretarza generalnego ONZ 12 września 2011 roku. Oba państwa wraz z Tadżykistanem i Uzbekistanem zwróciły w nim uwagę na potrzebę przygotowania w ramach ONZ dokumentu, który zawierałby podstawowe normy i zasady regulujące „zachowanie państw w przestrzeni informacyjnej”. Wśród zaproponowanych rozwiązań wymieniono m.in.:

- powstrzymanie się rządów od wykorzystania technologii informacyjnych i komunikacyjnych, w tym sieci, do wrogich działań lub aktów agresji,
- powstrzymanie się od rozpowszechniania „broni informacyjnych i związanych z [nimi — M.L.] technologii”,
- współpracę w zakresie zwalczania cyberprzestępczości i cyberterroryzmu, m.in. przez przeciwdziałanie rozpowszechnianiu informacji inspirujących postawy terrorystyczne, secesjonistyczne bądź radykalne, a także takie, które podważają polityczną, gospodarczą i społeczną stabilność państw,

[5] C. Riley: *China's military denies hacking allegations*. CNN, 20.02.2013: http://money.cnn.com/2013/02/20/technology/china-cyber-hacking-denial; dostęp: 26.02.2014.

[6] *Putin defies Convetion on Cybercrime*. CNEWS, 27.03.2008: http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913; dostęp: 26.02.2014.

[7] Y. Isakova: *Russia opts for universal anti-cybercrime convention*. The Voice of Russia, 20.07.2011: http://voiceofrussia.com/2011/07/20/53481702; dostęp: 26.02.2014.

- zapobieganie działaniom mającym na celu podważenie prawa państw do utrzymywania suwerennej kontroli nad technologiami informacyjnymi i komunikacyjnymi,
- potwierdzenie prawa państw do ochrony własnej przestrzeni informacyjnej oraz infrastruktury krytycznej,
- poszanowanie praw i wolności w przestrzeni informacyjnej,
- promocję koncepcji utworzenia wielostronnego, transparentnego, demokratycznego i międzynarodowego systemu zarządzania Internetem w celu zapewnienia sprawiedliwej dystrybucji zasobów, ułatwienia powszechnego dostępu do niego, a także zapewnienia jego stabilnego i bezpiecznego funkcjonowania,
- rozstrzyganie sporów wynikających z zastosowania wyżej wymienionych zasad w sposób pokojowy,
- wsparcie dla dwustronnej, regionalnej oraz międzynarodowej współpracy w tej dziedzinie, szczególnie w ramach ONZ, w procesie formułowania podstawowych norm i zasad pokojowego regulowania sporów oraz zwiększonej koordynacji w zakresie bezpieczeństwa informacyjnego (*Letter dated 12 September 2011*, 2011).

Warto podkreślić, iż list Rosji i Chin zawierał jedne z pierwszych tak kompleksowych propozycji uregulowania podstawowych zagadnień związanych ze szkodliwą aktywnością państw i podmiotów pozapaństwowych w cyberprzestrzeni.

Przedsięwzięcie to zostało zignorowane przez państwa zachodnie, w tym przede wszystkim Stany Zjednoczone, w które sposób zgoła odmienny podchodziły do tego typu zagadnień. Waszyngton, jakkolwiek był zwolennikiem rozwoju współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa, od lat prezentował jej odrębną wizję. Popierając inicjatywy zmierzające do zwalczania przestępczości komputerowej, czego wyrazem była kooperacja m.in. z Rosją w sprawie niektórych rezolucji Zgromadzenia Ogólnego ONZ, odnosił się dość sceptycznie do kolejnych prób uregulowania tak trudnych zagadnień, jak cyberwojna. Z jednej strony wyrazem tej polityki było więc wsparcie, jakiego USA udzieliło *Konwencji Rady Europy o cyberprzestępczości*, podpisując i ratyfikując ten dokument. Nie zgadzano się tym samym z wątpliwościami wobec tego traktatu formułowanymi m.in. przez Rosję czy przedstawicieli Międzynarodowego Związku Telekomunikacyjnego[8]. Z drugiej strony warto przywołać opinię Pashy Sharikova (2013: 2), który zauważył, iż sceptycyzm wobec propozycji rosyjsko-chińskich wynikał z odmiennej optyki samej istoty cyberbezpieczeństwa. Waszyngton postrzegał te zagadnienia w sposób zdecydowanie węższy, skupiając się głównie na ochronie infrastruktury teleinformatycznej lub krajo-

[8] B. Harley: *A Global Convention on Cybercrime?* „The Columbia Science and Technology Law Review" 23.03.2010: www.stlr.org/2010/03/a-global-convention-on-cybercrime; dostęp: 9.01.2013.

wych technologii przed wrogą lub nieuprawnioną manipulacją. Po drugie USA były zdania, iż regulacja Internetu powinna mieć ograniczony charakter, preferowano zatem podejście uwzględniające szeroko pojęty sektor prywatny oraz ośrodki badawcze. Kooperacja między różnymi rodzajami interesariuszy była tym samym sprzeczna z modelem hierarchicznym popieranym przez Moskwę i Pekin. Po trzecie Biały Dom był również oficjalnie przeciwny koncepcji „suwerenności w cyberprzestrzeni", której wdrożenie doprowadziłoby do wykształcenia zbyt statycznego systemu regulacji, co mogłoby zostać wykorzystane przez państwa autorytarne do tłumienia protestów opozycji lub łamania praw człowieka[9]. Po czwarte wydaje się, iż amerykański sceptycyzm wobec „traktatu o cyberwojnie" mógł wynikać również z chęci zabezpieczenia swojej przewagi technologicznej w cyberprzestrzeni. W tej sytuacji popieranie umowy zabraniającej użycia „cyberbroni" byłoby kontrproduktywne z perspektywy interesów USA. W efekcie na początku XXI wieku Stany Zjednoczone, jakkolwiek popierały rozmaite inicjatywy wymierzone w walkę z cyberprzestępczością, były postrzegane raczej jako „hamulcowy" inicjatyw mających przeciwdziałać konfrontacji państw w przestrzeni teleinformatycznej[10].

Różnicę zdań między stałymi członkami Rady Bezpieczeństwa ONZ najlepiej przedstawili Richard Clarke i Ron Deibert. Według Richarda Clarke'a „Stany Zjednoczone niemal w pojedynkę blokują kontrolę zbrojeń w cyberprzestrzeni. Rosja, nieco ironicznie, jest [jej — M.L.] głównym zwolennikiem. […] odkąd administracja Clintona jako pierwsza odrzuciła rosyjską propozycję, USA były stałym przeciwnikiem cyberkontroli zbrojeń" (za: Maurer, 2011: 20). Z kolei Ron Deibert z University of Toronto stwierdził:

> Rosja dążyła do kontroli zbrojeń w cyberprzestrzeni […]. Większość ludzi, z czym się zgadzam, postrzega to jako [działanie — M.L.] obłudne […], jako rosyjską próbę ograniczenia amerykańskiej przewagi w cyberdomenie. Rosja jest bardziej zaniepokojona kolorowymi rewolucjami oraz mobilizacją dysydentów oraz grup praw człowieka w Internecie — i stara się wyeliminować zdolność Stanów Zjednoczonych do wspierania tego typu społecznej mobilizacji — niż ochroną Internetu (Ibidem, s. 17).

Na tle powyższych różnic nie dziwi więc fakt, iż Rada Bezpieczeństwa ONZ pozostała w okresie pozimnowojennym bezczynna, jeśli chodzi o regulację zagadnień związanych z cyberbezpieczeństwem. Co prawda stanowisko Stanów

---

[9] M.D. Swaine: *Chinese Views on Cybersecurity in Foreign Relations*. Carnegie Endowment, s. 13—14: http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf; dostęp: 26.02.2014.

[10] Szerzej na temat priorytetów amerykańskiej polityki w tym zakresie: *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*. The White House, May 2011.

Zjednoczonych zaczęło ewoluować w trakcie prezydentury Baracka Obamy, który w sposób bardziej otwarty podchodził do wizji współpracy z Rosją i Chinami, nie osiągnięto jednak tutaj znaczącego przełomu na forum Organizacji Narodów Zjednoczonych[11].

W przeciwieństwie do RB ONZ organem głównym ONZ, który odgrywał na początku XXI wieku pewną rolę we współpracy międzynarodowej w dziedzinie bezpieczeństwa teleinformatycznego, była Rada Gospodarcza i Społeczna. Warto wymienić kilka jej najbardziej interesujących inicjatyw. Przede wszystkim w 2004 roku w rezolucji nr 26 powołała ona międzyrządowy zespół ekspertów odpowiedzialny za walkę z kradzieżą tożsamości online (*International Cooperation*, 2004). W 2007 roku ECOSOC przygotowała rezolucję nr 20, w której wezwano państwa członkowskie, aby dołączyły do *Konwencji Rady Europy o cyberprzestępczości* (*International Cooperation*, 2007). Jak wspomniano wyżej, temu stanowisku była jednak przeciwna Federacja Rosyjska. Rada tematykę cyberbezpieczeństwa poruszyła również w swoich pracach w 2009 roku, w rezolucji nr 22 (*International Cooperation*, 2009). W kwietniu 2011 roku przyjęła ona natomiast projekt rezolucji nr 20/7, w której wezwano Biuro NZ ds. Narkotyków i Przestępczości do kontynuowania i pogłębiania współpracy w zakresie zwalczania przestępczości komputerowej z innymi państwami, organizacjami międzynarodowymi, a także podmiotami sektora prywatnego[12]. W 2012 roku uchwalono dokument, w którym dokonano oceny skutków wprowadzania ustaleń ze Światowego Szczytu Społeczeństwa Informacyjnego (World Summit on the Information Society) (*Assessment of the progress*, 2012).

Oprócz rezolucji ECOSOC podejmowała inne inicjatywy, które w zamyśle miały promować współpracę międzynarodową w dziedzinie cyberbezpieczeństwa. Należy tu wymienić m.in.:

- wniosek wchodzącej w skład Rady Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości, która w 1999 roku zasugerowała podjęcie przez sekretarza generalnego ONZ badań nad przestępczością komputerową,

[11] Wyrazem tego było m.in. powołanie amerykańsko-rosyjskiej grupy roboczej ds. cyberbezpieczeństwa. Zob. *Fact Sheet: U.S. — Russian Cooperation on Information and Communication Technology Security*. Office of the Press Secretary. The White House, 17.07.2013: www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol; dostęp: 28.02.2014; *Joint Statement on the Inaugural Meeting of the U.S. — Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technology (ICT) in the Context of International Security*. Office of the Press Secretary. The White House, 22.11.2013: www.whitehouse.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi; dostęp: 28.02.2014.

[12] *Promotion of Activities Relating to Combating Cybercrime, Including Technical Assistance and Capacity-building*. ECOSOC Draft Resolution 20/7, April 2011: www.cfr.org/cybersecurity/ecosoc-draft-resolution-207-promotion-activities-relating-combating-cybercrime-including-technical-assistance-capacity-building/p28130; dostęp: 28.02.2014.

- apel Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości w 2004 roku o uchwalenie konwencji ONZ poświęconej cyberprzestępczości,
- raport Komisji z 2011 roku, w którym stwierdzono, iż Konwencja ONZ przeciwko transnarodowej przestępczości zorganizowanej (Convention against Transnational Organized Crime) odnosi się również do przestrzeni teleinformatycznej,
- raport Komisji ds. Środków Odurzających z 1999 roku, w którym omówiono m.in. wpływ Internetu na rosnącą popularność narkotyków,
- rezolucję Komisji ds. Środków Odurzających z 2005 roku, którą poświęcono prewencji zastosowania Internetu jako instrumentu przestępczości narkotykowej; sceptyczne stanowisko w tej sprawie zajęły Chiny (Maurer, 2011: 38—39),
- rozpoczęcie sesji Rady w 2010 roku od zaprezentowania raportu *Cyber security: emerging threats and challenges*, którego celem było przede wszystkim ukazanie potencjalnych możliwości budowy ram międzynarodowej współpracy w tej dziedzinie (*Cyber security*, 2010),
- zorganizowanie wraz z Międzynarodowym Związkiem Telekomunikacyjnym specjalnego spotkania poświęconego cyberbezpieczeństwu (*Special Event on Cybersecurity and Development*) w grudniu 2011 roku, którego celem było m.in. wypracowanie sposobów zwalczania przestępczości komputerowej oraz systemu dobrych praktyk[13].

Na tym tle widać więc wyraźnie, że ECOSOC mimo pozornie niewielkiego związku ze sprawami bezpieczeństwa teleinformatycznego od końca lat 90. XX wieku podejmowała starania, aby promować międzynarodową kooperację w tym zakresie, choć ich efekty w praktyce okazały się niewielkie.

Oprócz omówionych wyżej organów głównych w systemie ONZ funkcjonuje jednak szereg innych, które w różny sposób uwzględniały cyberbezpieczeństwo w swoich pracach. Przede wszystkim należy wskazać na utworzoną w 2005 roku przez sekretarza generalnego Antyterrorystyczną Zadaniową Grupę Realizacyjną (The Counter-Terrorism Implementation Task Force), która uzyskała ograniczone uprawnienia w tej dziedzinie na mocy zapisów *Globalnej strategii antyterrorystycznej Narodów Zjednoczonych* (*United Nations Global Counter-Terrorism Strategy*) z 2006 roku. Struktura ta składa się z 31 podmiotów międzynarodowych, w tym m.in.: INTERPOL-u, Biura ds. Rozbrojenia (Office for Disarmament Affairs) oraz Banku Światowego[14]. W jej ramach funkcjonuje Grupa Robocza ds. Przeciwdziałania Wykorzystaniu Internetu do Celów Terrorystycznych (Working Group on Countering the Use of Internet for Terrorist

[13] *Special Event on Cybersecurity and Development*. ECOSOC, 09.11.2011: www.un.org/en/ecosoc/cybersecurity; dostęp: 28.02.2014.

[14] Zob. też *Counter-Terrorism Implementation Task Force*. United Nations: www.un.org/en/terrorism/ctitf; dostęp: 28.02.2014.

Purposes), która jest odpowiedzialna m.in. za koordynację oraz badania, w jaki sposób poszczególne państwa członkowskie zwalczają cyberterroryzm[15].

Po drugie problematyką tą zajmuje się również Instytut Narodów Zjednoczonych ds. Badań Naukowych nad Rozbrojeniem (United Nations Institute for Disarmament Research). Pełni on funkcję ważnego forum dyskusyjnego, gdzie przedstawiciele środowiska naukowego oraz poszczególnych rządów wymieniają się opiniami na temat głównych zagrożeń teleinformatycznych i sposobów przeciwdziałania im. Warto podkreślić, iż w przeciwieństwie do ECOSOC dyskurs w ramach UNIDIR skupia się głównie na zagadnieniu szkodliwego wykorzystania cyberprzestrzeni przez państwa. Z jednej strony jego działalność przejawia się organizacją interesujących konferencji i seminariów naukowych, w tym m.in.: w 2008 roku na temat wpływu ICT na bezpieczeństwo międzynarodowe[16], w 2011 roku na temat cyberwojny[17], w 2012 roku na temat relacji pomiędzy cyberbezpieczeństwem a konfliktami zbrojnymi[18], w 2014 roku na temat zapobieganiu konfliktom w cyberprzestrzeni[19].

Z drugiej strony UNIDIR jest również źródłem wartościowych opracowań naukowych, w tym m.in.: *Increasing Access to Information Technology for International Security* (1997), które zostało poświęcone sposobom współpracy środowiska naukowego w dziedzinie bezpieczeństwa informacyjnego (Gasparini-Alves, ed., 1997), *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization* (2011) (Lewis, Timlin, 2011) czy *The Cyber Index. International Security Trends and Realities* (2013) (*The Cyber Index*, 2013).

Można wspomnieć również o roli Międzyregionalnego Instytutu Narodów Zjednoczonych ds. Badań nad Przestępczością i Wymiarem Sprawiedliwości (United Nations Interregional Crime and Justice Research Institute). Jako instytucja wspierająca organizacje rządowe i pozarządowe w ich działaniach na rzecz zwalczania przestępczości pełni ona tradycyjnie szereg funkcji, jest bowiem odpowiedzialna za zwiększanie zrozumienia problemów związanych z przestęp-

[15] *Working Group on Countering the Use of the Internet for Terrorist Purposes*. Counter-Terrorism Implementation Task Force: www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml; dostęp: 28.02.2014.

[16] *Information & Communication Technologies and International Security*. UNIDIR, 24—25.04.2008: www.unidir.org/programmes/emerging-security-threats/information-communication-technologies-and-international-security; dostęp: 28.02.2014.

[17] *Gearing Up for Cyberwar?* UNIDIR, 24.08.2011: www.unidir.org/programmes/emerging-security-threats/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building/gearing-up-for-cyberwar; dostęp: 28.02.2014.

[18] *Cybersecurity and Conflicts*. UNIDIR, 19.11.2012: www.unidir.org/programmes/emerging-security-threats/cybersecurity-and-conflicts; dostęp: 28.02.2014.

[19] *Cyber Stability Seminar 2014: Preventing Cyber Conflict*. UNIDIR, 10.02.2014: www.unidir.org/programmes/emerging-security-threats/cyber-stability-seminar-2014-preventing-cyber-conflict; dostęp: 28.02.2014.

czością, wzmacnianie skuteczności działań wymiarów sprawiedliwości, wsparcie dla poszanowania międzynarodowych instrumentów oraz innych standardów w tej dziedzinie oraz ułatwianie międzynarodowej współpracy[20]. W związku z tym Instytut od lat aktywnie zajmuje się problemami z zakresu bezpieczeństwa teleinformatycznego, skupiając się głównie na cyberprzestępczości i cyberterroryzmie. W tym celu w 2006 roku został zainicjowany program *Hackers Profile Project*, którego głównym założeniem było ułatwienie ich prewencji i zwalczania, a także podnoszenie skuteczności metod operacyjnych wykrywania sprawców. Składał się on z kilku faz, w tym m.in.: teoretycznej, obserwacyjnej, budowy bazy danych, identyfikacji hakerów oraz opracowania ich klasyfikacji[21]. Oprócz prac badawczych UNICRI pełni również funkcję ośrodka inspirującego międzynarodową debatę na temat cyberbezpieczeństwa. W listopadzie 2013 roku we Włoszech Instytut zorganizował np. „okrągły stół" poświęcony wpływowi przestępczości komputerowej na rozwój gospodarczy oraz działalność przedsiębiorstw[22].

Na tym tle można również wspomnieć o kilku inicjatywach ONZ, które skupiły się na szerszej kategorii bezpieczeństwa informacyjnego. Przede wszystkim należałoby zwrócić uwagę na sponsorowane przez Narody Zjednoczone Światowe Szczyty Społeczeństwa Informacyjnego (World Summit on the Information Society). Po raz pierwszy konferencja z tej serii, w której uczestniczyło 175 krajów, odbyła się w Genewie w dniach 10—12 grudnia 2003 roku. Przyjęto wówczas deklarację zasad oraz plan działań co do budowy światowego społeczeństwa informacyjnego. W pierwszym z tych dokumentów podkreślono potrzebę osiągnięcia równego dostępu do ICT, a także ich nieograniczonego zastosowania, opartego na pryncypiach Karty Narodów Zjednoczonych, Powszechnej Deklaracji Praw Człowieka czy Deklaracji Milenijnej. Z jednej strony zauważono, iż korzyści czerpane z tych technologii są wielowymiarowe oraz powinny mieć zasięg globalny. Omówiono tu np. ich rolę w dostępie do informacji i wiedzy, mediów czy kulturowej i językowej różnorodności, z drugiej jednak dostrzeżono szereg zagrożeń dla rozwoju społeczeństwa informacyjnego i podkreślono zasadniczą rolę, jaką w przeciwdziałaniu im mają do odegrania państwa członkowskie oraz sektor prywatny. Po drugie wskazano na fundamentalne znaczenie stabilnej i bezpiecznej infrastruktury teleinformatycznej. Po trzecie zaapelowano o opracowanie oraz implementację „globalnej kultury cyberbezpieczeństwa", co powinno wynikać głównie z większej intensyfikacji międzynarodowej współpracy w tej dziedzinie. Wyrażono ponadto poparcie dla innych inicjatyw Narodów Zjednoczonych, których celem było przeciwdziałanie szkodliwemu użyciu ICT (*Declaration of Principles*, 2003). W drugim z dokumentów wymieniono

[20] *About UNICRI*. UNICRI: www.unicri.it/institute; dostęp: 3.03.2014.

[21] *Cyber Threats*. UNICRI: www.unicri.it/special_topics/cyber_threats; dostęp: 3.03.2014.

[22] *Cyber crime: the risks for the economy and the enterprises*. UNICRI: www.unicri.it/in_focus/on/20131121_Cybercrime; dostęp: 3.03.2014.

natomiast podstawowe działania, jakie powinny podjąć rządy w celu budowy społeczeństwa informacyjnego. Wskazano tu m.in. na rozbudowę infrastruktury teleinformatycznej, promocję partnerstwa publiczno-prywatnego, ułatwienie dostępu do informacji i wiedzy, rozwijanie programów edukacyjnych i szkoleniowych oraz implementację nowych technologii w różnych dziedzinach życia (koncepcje *e-government*, *e-business*, *e-learning*, *e-science*, *e-health*). Stosunkowo dużo miejsca poświęcono również bezpieczeństwu teleinformatycznemu, wyodrębniając następujące priorytety:

- współpracę rządów z sektorem prywatnym, która powinna wykrywać cyberprzestępczość, a także zapobiegać i przeciwdziałać cyberprzestępczości oraz niewłaściwemu wykorzystaniu ICT,
- edukację i podnoszenie świadomości użytkowników na temat sposobów zapewnienia prywatności w sieci,
- zwalczanie spamu zarówno na poziomie narodowym, jak i międzynarodowym,
- dokonanie przeglądu krajowych regulacji prawnych dotyczących skutecznego użycia dokumentów oraz transakcji elektronicznych,
- wymianę dobrymi praktykami w tej dziedzinie,
- tworzenie ośrodków reagowania na incydenty teleinformatyczne oraz współpracę między nimi,
- zachęcanie państw do wzięcia udziału w innych inicjatywach ONZ w tej dziedzinie (*Plan of Action*, 2003).

Do drugiego Światowego Szczytu Społeczeństwa Informacyjnego doszło w listopadzie 2005 roku w Tunisie. Wśród najważniejszych podjętych wówczas decyzji należy wymienić przede wszystkim tę o powołaniu od 2006 roku Forum Zarządzania Internetem (Internet Governance Forum), które miało m.in. ułatwić wymianę informacji oraz dobrych praktyk, identyfikować narastające problemy i formułować związane z nimi rekomendacje czy przygotowywać sposoby przeciwdziałania wyzwaniom wynikającym z niewłaściwego zastosowania ICT (*Tunis Agenda*, 2005). Na tej kanwie społeczność międzynarodowa rozpoczęła wielowymiarowe wysiłki zmierzające do implementacji przyjętych w latach 2003—2005 założeń. Służyły temu takie inicjatywy, jak WSIS Forum, WSIS Stocktaking Process czy Partnership on Measuring ICT for Development[23].

Można także zwrócić uwagę na działania podejmowane przez wspomniane już grupy rządowych ekspertów, powołanych trzykrotnie przez sekretarza generalnego ONZ w celu analizy istniejących zagrożeń dla bezpieczeństwa teleinformatycznego. Pierwszy raport GGE (Governmental Group of Experts) został opublikowany w 2010 roku. Przygotowali go specjaliści z 15 państw, w tym m.in. z Białorusi, Brazylii, Chin, Niemiec, Indii, Izraela, Rosji, Wielkiej Bryta-

[23] *WSIS Implementation*. World Summit on the Information Society: www.itu.int/wsis/implementation.html; dostęp: 3.03.2014.

nii oraz Stanów Zjednoczonych. Do największych wyzwań zaliczono w nim rosnące zainteresowanie poszczególnych rządów wykorzystaniem ICT w charakterze nowych instrumentów prowadzenia wojny, działań wywiadowczych oraz środków nacisku politycznego (punkt II.7). W związku z tym wśród rekomendacji przyjętych przez grupę wymieniono pogłębienie dialogu między państwami na temat norm regulujących użycie technologii informacyjnych i komunikacyjnych (*Group of Governmental Experts*, A/65/201). W raporcie GGE z 2013 roku na problematykę rywalizacji i konfrontacji państw w cyberprzestrzeni położono jeszcze większy nacisk. W dokumencie tym, przygotowanym m.in. przez specjalistów z Argentyny, Kanady, Chin, Estonii, Francji, Rosji, Japonii i USA, zaakcentowano potrzebę ustalenia podstawowych norm i zasad zastosowania przez państwa technologii teleinformatycznych dla ochrony kluczowej infrastruktury krytycznej. Podkreślono również, że ICT powinny być używane wyłącznie w celach pokojowych. Raport skupił się jednak przede wszystkim na omówieniu nowych sposobów kooperacji państw oraz sektora prywatnego w celu zwalczania zagrożeń pojawiających się w sieci. Stwierdzono więc, że zastosowanie technologii informacyjnych i komunikacyjnych przez poszczególne rządy powinno być regulowane w oparciu o istniejące zapisy prawa międzynarodowego. Ponadto zauważono, że kraje członkowskie ONZ powinny intensywniej kooperować w zwalczaniu cyberprzestępczości i cyberterroryzmu, nie powinny także udostępniać swoich terytoriów podmiotom pozapaństwowym, wykorzystującym ICT w sposób niezgodny z prawem (*Group of Governmental Experts*, A/68/98). Warto przy tym odnotować zadowolenie amerykańskiej dyplomacji z zapisów tego raportu, był on bowiem potwierdzeniem stanowiska Departamentu Stanu, że normy prawa międzynarodowego, w tym *Karta Narodów Zjednoczonych*, powinny zachować moc sprawczą również w cyberprzestrzeni (Psaki, 2013).

Scharakteryzowane wyżej inicjatywy Organizacji Narodów Zjednoczonych można oceniać z dwóch perspektyw. Z jednej strony ONZ była jedną z pierwszych organizacji międzynarodowych, które zainteresowały się problematyką bezpieczeństwa teleinformatycznego. Podejmowane przez nią prace okazały się ważnym instrumentem podnoszenia świadomości społeczności międzynarodowej co do skali i specyfiki zagrożeń pojawiających się w cyberprzestrzeni. Za wartościowe w tym względzie należy uznać nie tylko przyjmowane od lat dokumenty koncepcyjne oraz rezolucje Zgromadzenia Ogólnego ONZ, ale również opracowania naukowe i przedsięwzięcia zmierzające do intensyfikacji globalnej debaty na ten temat. Z drugiej jednak strony należy stwierdzić, iż aktywność organizacji była z reguły wypadkową interesów poszczególnych państw członkowskich. Najbardziej wpływowe z nich, takie jak Stany Zjednoczone, Rosja oraz Chiny, sformułowały diametralnie różne priorytety w tym zakresie, co doprowadziło do skutecznego sparaliżowania wielu instytucji ONZ. Symbolem tej bezsilności stała się Rada Bezpieczeństwa, która mimo wyjątkowych kompetencji przez ponad dwie dekady nie zainteresowała się problemem cyberataków.

Jakkolwiek w ogólnikach niemal wszystkie rządy zgadzały się co do potrzeby efektywniejszego uregulowania zagadnień związanych z bezpieczeństwem teleinformatycznym, nie było konsensusu co do szczegółowych rozwiązań praktycznych. W okresie pozimnowojennym nie wykorzystano zatem drzemiącego w ONZ potencjału, aby doprecyzować istniejące już zapisy prawa międzynarodowego lub stworzyć nowe, odnoszące się wyłącznie do sfery cyberprzestrzeni.

5.2. Cyberzagrożenia w pracach Międzynarodowego Związku Telekomunikacyjnego[24]

Jedynym w zasadzie wyjątkiem od wyeksponowanej wyżej reguły jest Międzynarodowy Związek Telekomunikacyjny, będący jedną z najważniejszych organizacji wyspecjalizowanych w systemie ONZ. Ze względu na znaczenie Związku dla praktyki współpracy państw w dziedzinie bezpieczeństwa teleinformatycznego warto tę strukturę omówić osobno.

Na wstępie należałoby zauważyć, iż problematyką cyberbezpieczeństwa ITU zainteresował się dość późno, dopiero w 2001 roku, kiedy jego Rada zdecydowała o organizacji Światowego Szczytu Społeczeństwa Informacyjnego. W związku z omówionymi wcześniej ustaleniami WSIS Związek został uznany za organizację odpowiedzialną za wdrażanie przyjętych wówczas priorytetów z działów C2 (infrastruktura ICT) i C5 (bezpieczeństwo teleinformatyczne)[25]. To właśnie na tej podstawie ITU na początku XXI wieku zaangażował się w pogłębianie międzynarodowej współpracy państw w tej dziedzinie, zarówno w wymiarze koncepcyjnym, jak i *stricte* praktycznym.

Jeśli chodzi o wymiar koncepcyjny, dużą rolę odegrała tu przede wszystkim działalność Konferencji Pełnomocników Międzynarodowego Związku Telekomunikacyjnego. Na spotkaniu w Antalyi w 2006 roku w rezolucji nr 130 wyartykułowano np. potrzebę wzmocnienia roli ITU w zakresie „bezpieczeństwa wykorzystania technologii informacyjnych i komunikacyjnych", a także wypracowania dodatkowych rozwiązań i mechanizmów międzynarodowych, wykraczających poza literę *Konwencji Rady Europy o cyberprzestępczości* (*Strengthening the role of ITU*, 2006). Rezolucję nr 149 z 2006 roku poświęcono z kolei wypracowaniu podstawowej terminologii dotyczącej cyberbezpieczeństwa (*Study of definitions*, 2006). Ważną decyzję Konferencja podjęła również na

[24] Rozdział został opracowany na podstawie artykułu: Lakomy, 2013a.

[25] *ITU-T and WSIS (World Summit on the Information Society)*. International Telecommunication Union: www.itu.int/en/ITU-T/wsis/Pages/default.aspx; dostęp: 3.03.2014.

spotkaniu w Hyderabadzie w 2010 roku. Wówczas w rezolucji nr 69 wezwano państwa członkowskie do ustanowienia zespołów CIRT (Computer Incident Response Teams) oraz pogłębiania ich współpracy w oparciu o struktury Związku (*Creation of computer*, 2010). Szereg ciekawych rozwiązań koncepcyjnych przyjęto także na spotkaniu w Guadalajarze w 2010 roku. Można tutaj wymienić m.in.:

- rezolucję nr 130, w której zaakcentowano zasadnicze znaczenie cyberbezpieczeństwa w pracach Międzynarodowego Związku Telekomunikacyjnego (*Strengthening the role of ITU*, 2010),
- rezolucję nr 174 na temat podnoszenia świadomości państw członkowskich co do możliwych konsekwencji szkodliwego wykorzystania technologii informacyjnych i komunikacyjnych (*ITU's role*, 2010),
- rezolucję nr 179 poświęconą pogłębianiu współpracy państw członkowskich ITU dla ochrony dzieci w środowisku teleinformatycznym (*ITU's role in child online protection*, 2010),
- rezolucję nr 181 na temat terminologii z zakresu cyberbezpieczeństwa; przyjęto w niej jednoznaczną definicję tej kategorii (*Definitions and terminology*, 2010).

Oprócz Konferencji Pełnomocników ITU pewną aktywność przejawiało również Światowe Zgromadzenie Standardyzacji Telekomunikacji (World Telecommunication Standardization Assembly). Można tu wskazać m.in. na:

- rezolucję nr 52, przyjętą w październiku 2008 roku w Johannesburgu, którą poświęcono walce ze spamem w Internecie (*Countering and combating spam*, 2008),
- rezolucję nr 50, przyjętą w Dubaju w listopadzie 2012 roku, w której zaakceptowano szereg rozwiązań dotyczących różnych sposobów pogłębiania współpracy w zakresie cyberbezpieczeństwa w ramach ITU (np. wypracowania powszechnych standardów i wytycznych obrony przed cyberatakami oraz wykrywania ich sprawców) (*Cybersecurity*, 2012),
- rezolucję nr 52 poświęconą walce ze spamem przyjętą w Dubaju w 2012 roku (*Countering and combating spam*, 2012),
- rezolucję nr 58, przyjętą w Dubaju w 2012 roku, w której zadeklarowano wsparcie dla państw członkowskich w zakresie powoływania zespołów reagowania na incydenty komputerowe (CIRT) (*Encourage the creation*, 2012).

Można również wspomnieć o istotnych decyzjach podjętych przez Międzynarodową Konferencję Rozwoju Telekomunikacji. Świadczyły o tym m.in.:

- rezolucja nr 45 przyjęta na spotkaniu w Hyderabadzie w 2010 roku, w której uznano cyberbezpieczeństwo za jeden z priorytetów działalności Związku, proponując przy tym szereg mechanizmów współpracy międzynarodowej, dotyczących m.in. zwalczania spamu czy opracowania zestawu dobrych praktyk (*Mechanisms of enhancing*, 2010),

- rezolucja nr 69, również przyjęta na spotkaniu w Hyderabadzie, gdzie ponownie zaakcentowano potrzebę powoływania narodowych zespołów CIRT (*Creation of computer*, 2010).

Na tej podstawie widać więc wyraźnie, iż Międzynarodowy Związek Telekomunikacyjny od drugiej połowy pierwszej dekady XXI wieku na trwałe zainteresował się cyberbezpieczeństwem. W praktyce jego aktywność w tej dziedzinie została oparta przede wszystkim na zapisach Globalnej Agendy Cyberbezpieczeństwa (Global Cybersecurity Agenda). Warto szerzej omówić tę inicjatywę.

GCA została zainicjowana w 2007 roku przez sekretarza generalnego ITU Hamadouna Tourégo. Miała za zadanie ustanowić podstawowe ramy współpracy międzynarodowej na obszarze bezpieczeństwa teleinformatycznego w reakcji na decyzje podjęte przez Światowy Szczyt Społeczeństwa Informacyjnego (WSIS). Hamadoun Touré, inicjując ten program, stwierdził, że cyberbezpieczeństwo jest jednym z najważniejszych, globalnych zagadnień współczesności. Jego zdaniem w „erze informacyjnej" walka z cyberprzestępczością czy cyberterroryzmem wymaga „prawdziwie globalnego podejścia" (*Global Cybersecurity Agenda*, 2011: 4). Warto zauważyć, iż było to przedsięwzięcie, w które zaangażowało się wiele państw nieposiadających dotychczas dużych doświadczeń w tym wymiarze, patronami tej inicjatywy stali się bowiem były prezydent Kostaryki oraz noblista Óscar Arias Sánchez i prezydent Burkiny Faso Blaise Compaoré. W ramach GCA wyróżniono 7 celów strategicznych:

- przygotowanie strategii rozwoju modelowych rozwiązań prawnych zwalczania cyberprzestępczości, które byłyby możliwe do wprowadzenia na całym świecie,
- przygotowanie strategii budowy narodowych i regionalnych struktur organizacyjnych oraz polityk wymierzonych w przestępczość komputerową,
- określenie minimalnych standardów zabezpieczeń teleinformatycznych,
- budowa globalnych ram obserwacji, ostrzegania i reagowania na incydenty w cyberprzestrzeni,
- opracowanie uniwersalnego systemu cyfrowej tożsamości,
- przygotowanie strategii ułatwiającej rozwój instytucjonalnego oraz ludzkiego potencjału w tej dziedzinie,
- formułowanie propozycji co do ustanowienia ram globalnej, wielosektorowej strategii współpracy międzynarodowej (*GCA Strategy*, 2007: 1—2).

Działalność Globalnej Agendy Cyberbezpieczeństwa objęła pięć filarów: rozwiązania prawne, środki techniczne i proceduralne, struktury organizacyjne, budowę zdolności oraz międzynarodową kooperację.

Aktywność w ramach pierwszego filaru przewidywała przede wszystkim zlikwidowanie luk w systemach prawnych zarówno na poziomie narodowym, jak i międzynarodowym, co ułatwiłoby przeciwdziałanie przestępczości komputerowej. W tym celu ITU podjęło wysiłki na rzecz lepszego zrozumienia specyfiki tego procederu w krajach członkowskich. W założeniu miało to

pozwolić na harmonizację poszczególnych regulacji prawnych, a tym samym podnieść poziom cyberbezpieczeństwa w wymiarze globalnym. W związku z tym Międzynarodowy Związek Telekomunikacyjny przygotował kilka ważnych publikacji poświęconych tym zagadnieniom. Pierwsza z nich, *ITU Tookit for Cybercrime Legislation* opracowana w 2010 roku, składała się z kilku istotnych elementów. Przede wszystkim zawarto w niej propozycje podstawowych definicji w tej dziedzinie, w tym takich pojęć, jak *komputer*, *dostęp*, *dane komputerowe*, *program komputerowy*, *infrastruktura krytyczna*, *zniszczenia*, *zakłócenia*, *przejęcie*, *złośliwe oprogramowanie* czy *sieć*. Omówiono ponadto zagadnienia związane z jurysdykcją prawną w Internecie czy transgranicznym dostępem do danych komputerowych. Scharakteryzowano też ówczesny stan prawodawstwa w wybranych państwach na świecie (*ITU Toolkit*, 2010). Drugim ciekawym opracowaniem przygotowanym w ramach GCA w 2009 roku była publikacja *Understanding Cybercrime: A Guide for Developing Countries*. Zawarto w niej bardzo rozległą i ciekawą charakterystykę podstawowych zagrożeń bezpieczeństwa teleinformatycznego, w tym charakterystykę cyberprzestępczości (wraz z jej typologią), cyberterroryzmu oraz cyberwojny. Omówiono w niej podstawowe wyzwania związane z przeciwdziałaniem przestępczości komputerowej, zarówno w wymiarze praktycznym, jak i prawnym, scharakteryzowano funkcjonujące już strategie i dokumenty, także na poziomie międzynarodowym, oraz zasugerowano możliwe rozwiązania na przyszłość (*Understanding Cybercrime*, 2009). Można także wspomnieć o dokumencie *Understanding Cybercrime: Phenomena, Challenges and Legal Response* opublikowanym we wrześniu 2012 roku. Pogłębił on i zaktualizował spostrzeżenia zawarte we wcześniejszych publikacjach ITU na ten temat, charakteryzując zjawisko cyberprzestępczości oraz omawiając podstawowe sposoby jego zwalczania (*Understanding Cybercrime*, 2012).

Drugi filar Globalnej Agendy Cyberbezpieczeństwa został oparty głównie na aktywności Sektora Standaryzacyjnego Międzynarodowego Związku Telekomunikacyjnego (Standardization Sector — ITU-T). Działał on na rzecz nawiązania kontaktów państw z sektorem prywatnym, co miało prowadzić do harmonizacji polityk bezpieczeństwa teleinformatycznego i wykształcenia wspólnych wzorców. W związku z tym opracowano szereg propozycji obejmujących m.in. wymogi, porady i sugerowane rozwiązania, zarówno jeśli chodzi o wykrywanie, jak i zwalczanie cyberzagrożeń. Można tu wymienić takie ich zestawy, jak H.235 (dotyczące usług bazujących na IP), J.170 (ochrona komunikacji sieciowej), X.805 (bezpieczeństwo architektury sieciowej) czy X.1205 (poświęcona ogólnie zagrożeniom dla cyberbezpieczeństwa) (zob. np. *Overview of cybersecurity*, 2008). W ramach tego filaru funkcjonowanie rozpoczęła również grupa badawcza Study Group 17, która zajmowała się m.in. przygotowywaniem raportów i opracowań naukowych poświęconych bezpieczeństwu telekomunikacji (np. *Security in telecommunications and information technology*), wydawaniem

rekomendacji, a także wsparciem procesu tworzenia narodowych zespołów reagowania na incydenty komputerowe. Międzynarodowy Związek Telekomunikacyjny przyjął ponadto w 2007 roku mapę drogową budowy międzynarodowych standardów zabezpieczeń komputerowych (*ICT Security Standards Roadmap*), która składała się z listy organizacji standaryzacyjnych oraz ich działań w obszarze bezpieczeństwa teleinformatycznego, zaakceptowanych oraz jeszcze opracowywanych standardów, przyszłych potrzeb i propozycji oraz dobrych praktyk.

Do tego filaru można zaliczyć jeszcze dwie struktury: Globalne Centrum Odpowiedzi IMPACT (IMPACT Global Response Center) oraz Sektor Radiokomunikacji ITU (Radiocommunication Sector). Pierwsza z nich stała się największą bazą danych na temat zagrożeń teleinformatycznych (*Global Cybersecurity Agenda*, 2011: 18—26), druga natomiast była odpowiedzialna za przygotowanie standardów bezpieczeństwa w zakresie radiokomunikacji, a więc także takich rozwiązań, jak internet bezprzewodowy (3G)[26].

Trzeci filar Globalnej Agendy Cyberbezpieczeństwa obejmował działania na rzecz rozwoju struktur organizacyjnych. Można tu zwrócić uwagę na dwie grupy inicjatyw. Pierwszą były regionalne fora cyberbezpieczeństwa (Regional Cybersecurity Forums) organizowane przez Sektor Rozwoju ITU (ITU Development Sector) wraz z wybranymi interesariuszami. Ich głównym celem było zainicjowanie pierwszych kroków poszczególnych państw w kierunku budowy zdolności w tej dziedzinie. Przykładowo w 2009 roku w Tunisie doszło do takiego spotkania dla obszaru Afryki oraz państw arabskich. Poruszono wówczas m.in. kwestie ochrony infrastruktury krytycznej, ochrony sieci telekomunikacyjnych oraz opracowania narodowych strategii cyberbezpieczeństwa (*ITU Regional Cybersecurity*, 2009). Druga grupa działań była podejmowana przez Sekcję Zapewnienia Bezpieczeństwa IMPACT (IMPACT Security Assurance Division), która zajęła się przygotowywaniem globalnych wytycznych na obszarze bezpieczeństwa teleinformatycznego. Na zlecenie przeprowadzała także testy zabezpieczeń komputerowych (*Global Cybersecurity Agenda*, 2011: 28—29).

Czwarty filar zakładał rozwój zdolności państw członkowskich do zwalczania zagrożeń teleinformatycznych. Międzynarodowy Związek Telekomunikacyjny odwoływał się tu do kilku inicjatyw. Pierwszą z nich stanowił program narodowego cyberbezpieczeństwa (*ITU National Cybersecurity/CIIP Self-Assessment Tool*), którego celem był głównie przygotowanie rządów do ochrony teleinformatycznej infrastruktury krytycznej. Bazując na przeprowadzonej ocenie posiadanych przez dane państwo zdolności, ITU wspierało je w pracach nad narodową strategią cyberbezpieczeństwa, wskazując np. na najbardziej palące potrzeby i niedociągnięcia. Po drugie Związek starał się działać na rzecz budowy kultury cyberbezpieczeństwa w ramach inicjatywy *ITU Toolkit for Promoting a Culture*

[26] *ITU Radiocommunication Sector*. International Telecommunication Union: www.itu.int/ITU-R/index.asp?category=information&rlink=itur-welcome&lang=en; dostęp: 14.05.2014.

of Cybersecurity. Polegało to głównie na podnoszeniu świadomości wszystkich użytkowników ICT. Po trzecie powstał projekt *ITU Botnet Mitigation Toolkit*, którego celem była pomoc państwom rozwijającym się w zwalczaniu sieci *botnet*, które, jak wiadomo, mogą być wykorzystane do cyberataków typu DDoS. Po czwarte można wspomnieć o funkcjonowaniu dwóch struktur działających w ramach inicjatywy IMPACT: Centrum Szkolenia i Rozwoju Umiejętności (Training and Skills Development Centre) oraz Wydziału Badań (Research Divison) (Ibidem, s. 28—34).

Ostatni i zarazem najważniejszy filar GCA polegał na stymulacji międzynarodowej współpracy w dziedzinie cyberbezpieczeństwa. Należy w tym kontekście wspomnieć o tym, iż Międzynarodowy Związek Telekomunikacyjny starał się utrzymywać kontakty nie tylko z poszczególnymi państwami czy sektorem prywatnym, ale również z innymi organizacjami międzynarodowymi będącymi częścią systemu ONZ. Trzeba tu wymienić m.in. Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC), Instytut Narodów Zjednoczonych ds. Badań Naukowych nad Rozbrojeniem (UNIDIR), Fundusz Narodów Zjednoczonych na Rzecz Dzieci (UNICEF) czy Międzyregionalny Instytut Narodów Zjednoczonych ds. Badań nad Przestępczością i Wymiarem Sprawiedliwości (UNICRI). Ich przejawem był szereg interesujących przedsięwzięć. Przy współpracy z UNODC ITU podejmowało np. działania na rzecz walki z przestępczością komputerową, w tym głównie kradzieżą tożsamości online. Warto również wspomnieć o działalności Grupy Ekspertów Wysokiego Szczebla (High Level Expert Group — HLEG), będących przedstawicielami rządów, przemysłu, organizacji międzynarodowych czy szeroko pojętego środowiska naukowego. Do głównych zadań tej grupy powoływanej przez sekretarza generalnego Związku należały przede wszystkim prace analityczne, których rezultatem powinny być m.in. regularne aktualizacje Globalnej Agendy Cyberbezpieczeństwa (np. jej założeń). Międzynarodowy Związek Telekomunikacyjny zapoczątkował również program „Bramy cyberbezpieczeństwa" (*ITU Cybersecurity Gateway*), który stał się platformą wymiany informacji na temat narodowych, regionalnych i globalnych inicjatyw w tej dziedzinie (Ibidem, s. 36—39).

Oprócz scharakteryzowanej wyżej Globalnej Agendy Cyberbezpieczeństwa należy zwrócić szczególną uwagę jeszcze na dwa inne niezwykle ważne przedsięwzięcia świadczące o skuteczności ITU jako organizacji zajmującej się bezpieczeństwem teleinformatycznym. Pierwszym z nich było Międzynarodowe Wielostronne Partnerstwo Przeciwko Cyberzagrożeniom (International Multilateral Partnership Against Cyber Threats — IMPACT), z którym ITU nawiązało współpracę w 2008 roku. W 2011 roku stało się ono *de facto* ciałem wykonawczym Związku na obszarze cyberbezpieczeństwa[27]. Jak stwierdzono na stronie

[27] *Impact — International Multilateral Partnership Against Cyber Threats*. s. 4—5: www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT_AnnualBook.pdf; dostęp: 7.03.2014.

internetowej Międzynarodowego Związku Telekomunikacyjnego, był to pierwszy w historii globalny, wielowymiarowy, publiczno-prywatny sojusz wymierzony w zwalczanie zagrożeń ICT skupiający w 2014 roku 149 państw świata, w tym 44 z Azji i Australii, 51 z Afryki, 15 z Europy Wschodniej, 14 z Europy Zachodniej oraz 25 z obu Ameryk. Co niezwykle ciekawe, nie było wśród nich Stanów Zjednoczonych i Federacji Rosyjskiej, w programie partycypowała natomiast Chińska Republika Ludowa[28]. Zgodnie z tłumaczeniami administracji amerykańskiej głównym powodem sceptycyzmu USA była obecność w tej inicjatywie takich „państw zbójeckich", jak Syria czy Iran[29]. Na tym tle IMPACT zyskała bardzo szerokie kompetencje, obejmujące m.in. ocenę wrażliwości systemów teleinformatycznych, przeprowadzanie zewnętrznych i wewnętrznych testów penetracyjnych, ocenę aplikacji internetowych, publikowanie alarmów i ostrzeżeń o zagrożeniach, reagowanie na incydenty teleinformatyczne, prewencję wycieku danych, a także prowadzenie programów szkoleniowych i edukacyjnych[30].

Realizując założenia Globalnej Agendy Cyberbezpieczeństwa, w ramach ITU-IMPACT powołano cztery ważne struktury:

1. Globalne Centrum Odpowiedzi (Global Response Centre), które w oparciu o współpracę zarówno z państwami członkowskimi, jak i z korporacjami zajmującymi się zabezpieczeniami komputerowymi (F-Secure, Trend Micro, Microsoft, Symantec Corporation, Kaspersky Lab) udostępnia „system wczesnego ostrzegania" o incydentach komputerowych — Network Early Warning System (NEWS). NEWS nie tylko na bieżąco monitoruje w czasie rzeczywistym (*real-time*) zagrożenia pojawiające się w cyberprzestrzeni, ale także dokonuje ich oceny, analizy oraz doradza członkom, w jaki sposób należy je zwalczać[31]. Ponadto w ramach GRC powstały centrum analizy złośliwego oprogramowania oraz platforma wymiany doświadczeń i opinii ekspertów z całego świata (Electronically Secure Collaboration Application Platform for Experts — ESCAPE). GRC udostępnia szereg innych usług, wśród których należy wymienić zaumatyzowany system analizy zagrożeń (Automated Threat Analysis System — ATAS) czy bazy danych istniejących już zagrożeń teleinformatycznych. W tym kontekście warto zauważyć, iż Globalne Centrum Odpowiedzi IMPACT stało się na przełomie XX i XXI wieku

[28] *ITU-IMPACT*. International Telecommunication Union: www.itu.int/en/ITU-D/Cybersecurity/Pages/ITU-IMPACT.aspx; dostęp: 7.03.2014.

[29] J. Westby: *U.S. Administration's Reckless Cyber Policy Puts Nation at Risk*. „Forbes", 04.06.2012: www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk; dostęp: 7.03.2014.

[30] Zob. *Service Catalogue 2011—2012*. ITU-IMPACT: www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_IMPACT_Service_Catalogue_Rev2.pdf; dostęp: 7.03.2014.

[31] Odnosząc to do rozważań z poprzednich rozdziałów, należy pamiętać, iż nie jest to do końca system „wczesnego" ostrzegania, reaguje bowiem na zagrożenia, które już w cyberprzestrzeni zaistniały (*post factum*).

jedną z najważniejszych instytucji w wymiarze globalnym, które udowodniły, na czym powinna w praktyce polegać międzynarodowa współpraca na obszarze cyberbezpieczeństwa[32].

2. Centrum dla Polityki i Współpracy Międzynarodowej (Centre for Policy & International Cooperation), które stanowi platformę pogłębiania i intensyfikowania kontaktów podmiotów sektora publicznego i prywatnego zmierzających do globalnej harmonizacji prawodawstwa dotyczącego przestępczości komputerowej, podnoszenia świadomości użytkowników Internetu, łagodzenia skutków ataków teleinformatycznych, a także ochrony dzieci w środowisku sieciowym. Wśród podejmowanych przez Centrum inicjatyw można wymienić m.in. współpracę z INTERPOL-em, którą rozpoczęto w maju 2011 roku, organizację szeregu spotkań i konferencji międzynarodowych (np. Honeynet Project Workshop w lutym 2009 roku w Kuala Lumpur czy ITU-IMPACT Partner Forum) lub program ochrony dzieci online (Children Online Protection — COP)[33].
3. Centrum Szkolenia i Rozwoju Umiejętności (Centre for Training & Skills Development) oferujące światowej klasy kursy specjalizacyjne w dziedzinie cyberbezpieczeństwa. Organizuje ono również seminaria oraz warsztaty dla ekspertów przy współpracy z ośrodkami badawczymi, korporacjami czy organizacjami międzynarodowymi. Można tu wymienić m.in. *IMPACT-Microsoft Regional Critical Infrastructure Protection Seminar* czy *SANS-IMPACT Hacker Techniques, Exploits and Incident Handling Training*. W obu przypadkach zostały one przeprowadzone w Cyberjayi w Malezji. Ponadto CTSD prowadzi program stypendialny przeznaczony dla specjalistów z krajów rozwijających się. Warto dodać, iż lista prowadzonych przez Centrum szkoleń jest bardzo szeroka i obejmuje takie propozycje, jak kurs etycznego hakera czy administratora sieci komputerowej[34].
4. Centrum ds. Badań i Zapewnienia Bezpieczeństwa (Centre for Security Assurance & Research) zajmujące się przede wszystkim wypracowywaniem nowych rozwiązań na obszarze bezpieczeństwa teleinformatycznego oraz

---

[32] *Global Response Center*. International Multilateral Partnership Against Cyber Threats: www.impact-alliance.org/services/grc-introduction.html; dostęp: 7.03.2014; *Impact — International Multilateral Partnership Against Cyber Threats*…, op.cit., s. 9; *Global Response Center — Technical Note*. International Multilateral Partnership Against Cyber Threats: www.itu.int/ITU-D/cyb/cybersecurity/docs/Technical_Note.pdf; dostęp: 7.03.2014.

[33] *Impact — International Multilateral Partnership Against Cyber Threats*..., op.cit., s. 11—14; *Center for Policy & International Cooperation*. International Multilateral Partnership Against Cyber Threats: www.impact-alliance.org/services/centre-for-policy-policy.html; dostęp: 7.03.2014.

[34] *Centre for Training & Skills Development*. International Multilateral Partnership Against Cyber Threats: www.impact-alliance.org/services/centre-for-training-overview.html; dostęp: 7.03.2014; *Impact — International Multilateral Partnership Against Cyber Threats*…, op.cit., s. 22—27.

testowaniem tych już istniejących. Centrum oferuje szereg usług, do których należy zaliczyć przede wszystkim IGSS (*IMPACT Government Security Scorecard*), który polega na prowadzeniu audytów wybranej rządowej infrastruktury czy aplikacji pod kątem posiadanych przez nie luk i błędów. CSAR prowadzi także program *CIRT-Lite*, którego celem jest pomoc państwom członkowskim w tworzeniu pierwszych narodowych zespołów reagowania na incydenty komputerowe. Wzięły w nim dotychczas udział takie państwa, jak Afganistan, Nigeria, Serbia, Malediwy czy Mali. Można także wspomnieć o programie ALERT (*Applied Learning for Emergency Response Teams*), polegającym na utrzymywaniu i podnoszeniu zdolności i kompetencji narodowych zespołów reagowania na incydenty komputerowe za pomocą ćwiczeń realizowanych w cyberprzestrzeni[35].

Drugim wyjątkowym przedsięwzięciem podjętym przez Międzynarodowy Związek Telekomunikacyjny stał się wspomniany już program ochrony dzieci online (COP). Miał on na celu identyfikację zagrożeń dla małoletnich w cyberprzestrzeni, podnoszenie świadomości, wypracowanie narzędzi minimalizowania ryzyka dla dzieci online, wymianę doświadczeń i wiedzy w tym zakresie. W założeniu program ten miał więc za zadanie zintensyfikować międzynarodową współpracę zmierzającą do ochrony najmłodszych użytkowników technologii informacyjnych i komunikacyjnych. W jego ramach ITU nawiązało dialog z takimi podmiotami, jak UNICEF, UNIDIR, UNICRI czy Komisja Europejska[36].

Wszystkie wskazane wyżej przykłady sugerowałyby więc, iż Międzynarodowy Związek Telekomunikacyjny skupiał się na walce z cyberprzestępczością oraz cyberterroryzmem, pomijał natomiast zagadnienia, które regularnie budziły kontrowersje i spory w środowisku międzynarodowym. Chodziło tu głównie o problem wykorzystania instrumentów teleinformatycznych przez poszczególne państwa. Można jednak wskazać na kilka wyjątków od tej reguły. Przede wszystkim za taki należy uznać propozycję osiągnięcia globalnego „cyberpokoju" wysuniętą wspólnie ze Światową Federacją Naukowców (World Federation of Scientists). W styczniu 2011 roku obie organizacje wydały wspólną publikację pod tytułem *The Quest for Cyber Peace*, której jednym z autorów był sekretarz generalny ITU Hamadoun Touré. Zawarł on tam szereg interesujących pomysłów, w jaki sposób zapewnić pokój i stabilność w cyberprzestrzeni. Na wstępie podkreślił on rosnące zagrożenie wystąpieniem zjawiska cyberwojny. Przywołując przykłady Estonii, Gruzji, Korei Południowej czy Stanów Zjednoczonych, wskazał na narastające wyzwania dla bezpieczeństwa

[35] *Impact — International Multilateral Partnership…*, op.cit., s. 30—32; *Centre for Security Assistance & Research, International Multilateral Partnership Against Cyber Threats*. IMPACT: www.impact-alliance.org/services/centre-for-security-igss.html; dostęp: 7.03.2014.

[36] *Child Protection Online*. International Telecommunication Union: www.itu.int/osg/csd/cybersecurity/gca/cop/index.html; dostęp: 7.03.2014.

narodowego i międzynarodowego, wynikające z cyberataków (Touré, 2011a: 7—13). Jego zdaniem postulowany stan mógł zostać więc osiągnięty w oparciu o 5 zasad:

1. Każdy rząd powinien zapewnić swoim obywatelom dostęp do komunikacji.
2. Każdy rząd powinien ochraniać swoich obywateli w cyberprzestrzeni.
3. Żadne państwo nie powinno udzielać schronienia przestępcom i terrorystom na swoim terytorium.
4. Żadne państwo nie powinno jako pierwsze dokonywać cyberataków na inne kraje.
5. Każde państwo powinno zobowiązać się do współpracy z resztą społeczności międzynarodowej w celu zagwarantowania pokoju w cyberprzestrzeni (Touré, 2011b: 103).

W tej samej publikacji zawarto również ważną deklarację Światowej Federacji Naukowców: *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. Stwierdzając w niej narastające uzależnienie człowieka od technologii informacyjnych i komunikacyjnych oraz zauważając wynikające z tego wyzwania, zaproponowano szereg zasad, na których miałby opierać się „cyberpokój":

1. Wszystkie państwa powinny uznać, że prawo międzynarodowe gwarantuje wolny przepływ informacji i idei, także w wymiarze online.
2. Państwa powinny razem opracować wspólny kodeks postępowania oraz zharmonizowane, globalne ramy prawne dla cyberprzestrzeni. Państwa, dostawcy internetowi oraz użytkownicy sieci powinni wspierać międzynarodowe wysiłki na rzecz zwalczania cyberprzestępczości.
3. Wszyscy użytkownicy, dostawcy internetowi oraz państwa powinni przeciwdziałać wykorzystaniu cyberprzestrzeni w sposób szkodliwy, szczególnie przeciwko dzieciom.
4. Interesariusze (państwa, organizacje, sektor prywatny) powinni wprowadzić i utrzymywać kompleksowe programy ochrony, bazujące m.in. na globalnie uznanych standardach i dobrych praktykach.
5. Producenci oprogramowania i sprzętu komputerowego powinni dążyć do rozwoju bezpiecznych i elastycznych technologii.
6. Rządy powinny aktywnie uczestniczyć w pracach Organizacji Narodów Zjednoczonych zmierzających do osiągnięcia cyberbezpieczeństwa i cyberpokoju, a także unikać wykorzystania cyberprzestrzeni w konfliktach[37].

W dużej mierze założenia tej deklaracji pokrywały się więc z propozycjami sekretarza generalnego ITU. W tym kontekście warto również przytoczyć słowa znajdujące się w podsumowaniu opracowania pod redakcją Hamadouna Touréго. Zawarto tam niezwykle ważne pytanie:

[37] *Erice Declaration of Principles for Cyber Stability and Cyber Peace*. In: *The Quest for Cyber Peace*. Ed. H.I. Touré. Geneva 2011, s. 111.

> Dlaczego cyberpowstrzymywanie i cyberpokój nie są codzienną mantrą? W zamian dowódcy wojskowi na całym świecie są zajęci ogłaszaniem powstawania cyberdowództw oraz ich planów […]. Gdy kraje stanęły w obliczu broni atomowej, zaczęły domagać się [jej — M.L.] powstrzymania i nieproliferacji. Państwa na całym świecie połączyły się we wspólnej sprawie zatrzymania globalnego zagrożenia dla ludzkości […]. Jakkolwiek wiele międzynarodowych organizacji pracuje nad różnymi aspektami cyberprzestępczości i/lub cyberkonfliktów, tylko ITU przyjęła globalną optykę […]. Mamy nadzieję, że inne organizacje będą popierać i naśladować to podejście, a ich przywódcy poczynią kroki w celu opracowania cyberkodu postępowania oraz ram prawnych, które będą wspierały i rozwijały geo-cyber-stabilność (Westby, 2011: 112—113).

O zainteresowaniu władz Międzynarodowego Związku Telekomunikacyjnego fenomenem cyberwojny świadczyły inne wypowiedzi sekretarza generalnego. Już w 2009 roku na konferencji Telecom World w Genewie Touré stwierdził: „można łatwo zgadnąć, że kolejna wojna światowa będzie się toczyła w cyberprzestrzeni, a my musimy temu zapobiec". Ponadto dodał, że ze względu na stopień uzależnienia różnych sfer życia człowieka od ICT konsekwencje tej wojny byłyby „katastrofalne". W związku z tym zapowiedział, że Związek będzie podejmował starania na rzecz budowy międzynarodowych ram prawnych, które pozwoliłyby na uregulowanie tych kwestii, m.in. poprzez zasadę powstrzymania się od pierwszego uderzenia w cyberprzestrzeni[38]. Do tych słów sekretarz generalny ITU nawiązywał i później. W jednym z kolejnych wystąpień Hamadoun Touré zauważył, iż międzynarodowa cyberwojna byłaby „gorsza niż tsunami". W związku z tym jego marzeniem było przyjęcie globalnego traktatu o „cyberpokoju", który zapobiegłby takiemu scenariuszowi. Jak jednak zaznaczył, jego pomysły w tej materii spotykały się ze stałym oporem ze strony wielu państw uprzemysłowionych[39]. W innej wypowiedzi z 2010 roku na konferencji w Hyderabadzie wrócił do już wcześniej sformułowanych założeń polityki cyberbezpieczeństwa Związku. Zaproponował wprowadzenie dwóch zasad, wspólnych dla całej społeczności międzynarodowej: według pierwszej każdy kraj powinien powstrzymywać się od rozpoczynania konfliktu w cyberprzestrzeni (zasada *no first attack*), według drugiej rządy nie powinny udzielać sprawcom ataków komputerowych schronienia na swoim terytorium. Warto jednak zaznaczyć, iż sugestie te nie miały charakteru oficjalnej propozycji skierowanej do państw członkowskich (Maurer, 2011: 30).

Władzom Międzynarodowego Związku Telekomunikacyjnego w kolejnych latach nie udało się tymi pomysłami zainteresować większości krajów członkow-

[38] R. Field: *ITU targets cyber warfare*. ITP.net, 06.10.2009: www.itp.net/577842-itu-targets-cyber-warfare; dostęp: 10.03.2014.

[39] D. Meyer: *ITU Head: Cyberwar could be 'worse than tsunami'*. ZDNet, 03.09.2010: www.zdnet.com/itu-head-cyberwar-could-be-worse-than-tsunami-3040089995; dostęp: 10.03.2014.

skich. W związku z tym Hamadoun Touré po 2010 roku zaczął o wiele rzadziej poruszać problem cyberwojny. Co prawda nawiązał do tego m.in. na spotkaniu w Erice w sierpniu 2012 roku[40], nie przełożyło się to jednak na żadne praktyczne przedsięwzięcia, wzorowane chociażby na ITU-IMPACT czy GCA. Bezczynność w tej materii wynikała, jak wspomniano, ze sprzeciwu części państw rozwiniętych. Choć Touré nigdy nie sprecyzował, o które z nich mu chodziło, można tu wskazać na Stany Zjednoczone, krytycznie odnoszące się do tego typu postulatów. Było to tym bardziej ewidentne, iż był on w Waszyngtonie uznawany za polityka wspierającego głównie rosyjską wizję rozwoju współpracy międzynarodowej. Jak stwierdził Tom Gjelten, wybór na stanowisko zawdzięczał zresztą w dużej mierze właśnie Moskwie[41].

Różnice między państwami członkowskimi stały się niezwykle wyraźne również podczas prac Międzynarodowego Związku Telekomunikacyjnego nad nowym traktatem regulującym funkcjonowanie systemów telekomunikacyjnych (*International Telecommunication Regulations* — ITR). Głównym zamiarem ITU było zaktualizowanie wcześniejszego dokumentu tego typu, uchwalonego jeszcze w 1988 roku w ramach WATTC (World Administrative Telegraph and Telephone Conference)[42]. Warto zaznaczyć, iż jeszcze przed rozpoczęciem prac na konferencji w Dubaju w grudniu 2012 roku nowy traktat wywoływał ogromne kontrowersje, głównie wśród zaawansowanych technologicznie państw i społeczeństw zachodnich. Można wskazać na kilka przykładów tego stanu rzeczy. Po pierwsze swoje obiekcje związane z planami regulacji Internetu zgłosiła Unia Europejska. Parlament Europejski w rezolucji z listopada 2012 roku stwierdził, iż Międzynarodowy Związek Telekomunikacyjny nie powinien mieć możliwości autorytatywnego wpływu na funkcjonowanie globalnej sieci. Wskazując na brak transparentności prowadzonych negocjacji na ten temat, zauważono, iż propozycje ITU mogłyby zagrozić otwartemu i konkurencyjnemu charakterowi Internetu. W związku z tym PE wyraził opinię, iż dotychczasowe regulacje ITR, jak również uprawnienia Międzynarodowego Związku Telekomunikacyjnego, powinny zostać utrzymane bez zmian[43]. Stanowisko to poparła zresztą wiceprzewodnicząca Komisji Europejskiej Neelie Kroes, która zaakcentowała w swojej wiadomości zamieszczonej na portalu Twitter, iż nie powinno się naprawiać czegoś, co nie jest zepsute[44]. Po drugie ostry sprzeciw wyraziła amerykańska korpo-

[40] H.I. Touré: *The Role of Science in the Third Millenium. Cyber Resilience: The Essence of Cyber Peace*. Erice International Seminars on Planetary Emergencies, Erice 20.08.2012: www.itu.int/en/osg/speeches/Pages/2012-08-20.aspx; dostęp: 10.03.2014.

[41] T. Gjelten: *Shadow Wars: Debating 'Cyber Disarmament'*. „World Affairs", November/December 2010: www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament; dostęp: 10.03.2014.

[42] *What are the ITRs?* Internet Society: www.internetsociety.org/itr; dostęp: 10.03.2014.

[43] *European Parliament on the forthcoming World Conference*, 2012.

[44] N. Kroes: *The internet works*. Twitter: https://twitter.com/NeelieKroesEU/status/274071153597546496; dostęp: 10.03.2014.

racja Google, która uznała ruch ITU za zagrożenie dla wolnego i niezależnego Internetu, według niej bowiem mógł on w rezultacie doprowadzić do ocenzurowania przez niektóre rządy treści zamieszczanych online. Skrytykowano także pominięcie w negocjacjach wielu grup interesariuszy, w tym głównie przedstawicieli sektora prywatnego. W związku z tym Google zainicjował akcję sprzeciwu, którą poparło niemal 3 miliony internautów[45]. Po trzecie podobne stanowisko zajął amerykański Kongres, który 5 grudnia 2012 roku przyjął jednomyślnie rezolucję potępiającą ITU za pomysł aktualizacji dotychczasowych regulacji telekomunikacyjnych. Stwierdzono w niej, iż Stany Zjednoczone opowiadają się za otwartą strukturą Internetu oraz podejściem uwzględniającym mnogość interesariuszy w tej dziedzinie, co leżało u podstaw rozwoju tej domeny od jej zarania[46]. Można również wymienić całą gamę innych podmiotów opowiadających się zdecydowanie przeciwko inicjatywie Związku, w tym m.in.: Electronic Frontier Foundation, Human Rights Watch, Anonymous, Valve czy Center for Democracy and Technology. W sumie swój sprzeciw wyraziło ponad 1500 organizacji ze 190 krajów świata[47].

Ostre kontrowersje i spory uwidoczniły się podczas właściwych negocjacji prowadzonych zarówno przed konferencją w Dubaju, jak i w jej trakcie w dniach 3—14 grudnia 2012 roku. Wynikały one w głównej mierze z prób uwzględnienia w ITR zagadnień związanych z regulacją Internetu wbrew wcześniejszym zapewnieniom władz ITU[48]. Z jednej strony podczas szczytu wyodrębniła się grupa państw zachodnich na czele ze Stanami Zjednoczonymi, które wyrażały swój sceptycyzm wobec szeregu propozycji wysuniętych przez władze organizacji. Przedstawiciel USA Terry Kramer postrzegał je wręcz w kategoriach zagrożenia dla praw człowieka w Internecie oraz wartości demokratycznych, negatywnie podchodził również do rosyjskich postulatów zwiększonego wpływu poszczególnych krajów na funkcjonowanie cyberprzestrzeni. W tym kontekście w mediach zachodnich pojawiły się komentarze, które jednoznacznie wskazywały, iż jednym z powodów amerykańskiego sprzeciwu była sympatia sekretarza generalnego ITU wobec polityki Federacji Rosyjskiej. Zdaniem wielu dziennikarzy celem Kremla było przeniesienie części kompetencji do regulowania globalnej sieci z ciał zdominowanych przez USA (takich jak ICANN) na rzecz bardziej przyjaznego Moskwie Międzynarodowego Związku Telekomuni-

[45] *Take Action*. Google: www.google.com/intl/en/takeaction/whats-at-stake; dostęp: 10.03.2014.

[46] N. McAllister: *Entire US Congress votes against ITU control of internet*. „The Register" 05.12.2012: www.theregister.co.uk/2012/12/05/us_votes_against_itu_internet_control; dostęp: 10.03.2014.

[47] *Protect Global Internet Freedom*: www.protectinternetfreedom.net; dostęp: 10.03.2014.

[48] Szerzej na temat przebiegu negocjacji w: M. Mueller: *What really happened in Dubai?* Internet Governance Project, 13.12.2012: www.internetgovernance.org/2012/12/13/what-really-happened-in-dubai; dostęp: 13.08.2014.

kacyjnego[49]. Unia Europejska, która czerpała dotychczas korzyści z takiej sytuacji, zmianę *status quo* również uznawała za poważne zagrożenie dla swoich interesów. Warto dodać, iż na konferencji w Dubaju miały zostać również podjęte próby omówienia podstawowych zagadnień związanych z globalnym cyberbezpieczeństwem. Postulaty tego typu wysuwała właśnie Federacja Rosyjska, czemu ostro sprzeciwiał się Biały Dom[50].

Jak można się było spodziewać, szczyt ITU poniósł *de facto* porażkę: opracowano wprawdzie zaktualizowaną wersję ITR, w której podkreślono m.in. suwerenne prawo poszczególnych rządów do regulowania swoich sieci telekomunikacyjnych[51], wyodrębniła się jednak duża grupa państw, które nie zgodziły się na zaproponowane rozwiązania. Na 144 uczestników konferencji nowe ITR zaakceptowało jedynie 89, odmówiły tego natomiast takie kraje, jak Stany Zjednoczone, Kanada, Wielka Brytania, Szwecja, Holandia, Republika Czeska oraz Dania[52]. W ciekawy sposób wszystkie powyższe kontrowersje oraz ich przyczyny podsumował Adam Popescu. Wymienił on 5 podstawowych powodów, przez które Waszyngton nie zdecydował się na podpisanie dokumentu. Jego zdaniem wynikało to przede wszystkim z zastosowania dwuznacznej terminologii, szczególnie jeśli chodzi o podmioty funkcjonujące w cyberprzestrzeni. Po drugie sprzeciwiano się pomysłom walki ze spamem, co w opinii administracji Obamy oznaczałoby pierwszy krok w stronę ograniczenia wolności słowa online. Po trzecie USA krytykowało pomysł uwzględnienia kwestii związanych z bezpieczeństwem teleinformatycznym. Po czwarte sprzeciwiano się pomysłom globalnej kontroli Internetu, wychodząc z założenia, iż żaden pojedynczy podmiot nie powinien posiadać takich zdolności. Po piąte ITR wbrew zapowiedziom Hamadouna Tourégo dotyczył głównie regulacji Internetu[53].

Omówione wyżej wydarzenia stały się więc kolejnym dowodem na to, iż społeczność międzynarodowa podzieliła się na dwa obozy mające odmienne pomysły co do kierunku dalszej współpracy w dziedzinie cyberbezpieczeństwa. Pierwszy, składający się głównie ze Stanów Zjednoczonych wraz z sojusznikami europejskimi, w dużej mierze opowiadał się za utrzymaniem *status quo*, sprze-

---

[49] L. Kelion: *UN internet regulation treaty talks begin in Dubai*. BBC News, 03.12.2012: www.bbc.com/news/technology-20575844; dostęp: 10.03.2014.

[50] J. Blau: *Battle Growing Over International Internet Regulation*. „IEEE Spectrum" 30.11.2012: http://spectrum.ieee.org/telecom/internet/battle-brewing-over-international-internet-regulation; dostęp: 10.03.2014.

[51] *Final Acts World Conference*, 2012.

[52] *A digital cold war?* „The Economist" 14.12.2014: www.economist.com/blogs/babbage/2012/12/internet-regulation; dostęp: 10.03.2014; *WCIT collapses: US, UK, allies refuse to sign treaty after Africa wins floor vote*. Commsday.com, 14.12.2012: www.commsday.com/uncategorized/wcit-collapses-us-uk-allies-refuse-to-sign-treaty-after-africa-wins-floor-vote; dostęp: 10.03.2014.

[53] A. Popescu: *5 Reasons Why The U.S. Rejected The ITU Treaty*. ReadWrite.com, 14.12.2012: http://readwrite.com/2012/12/14/5-reasons-why-the-us-rejected-the-itu-treaty; dostęp: 10.03.2014.

ciwiając się wszelkim inicjatywom, które mogłyby zwiększyć kontrolę poszczególnych państw nad narodowymi elementami cyberprzestrzeni. Ponadto USA wyrażały swój sceptycyzm wobec jakichkolwiek pomysłów podpisania międzynarodowego traktatu dotyczącego zjawiska cyberwojny. Druga grupa, na której czele stały Rosja oraz Chiny, zajmowała zdecydowanie odmienne stanowisko. Moskwa i Pekin nie tylko pragnęły uzyskać większą kontrolę nad Internetem, lecz podkreślały także potrzebę osiągnięcia globalnego porozumienia w sprawie ograniczenia rywalizacji państw w tej sferze. Na tym tle nie dziwią więc głosy określające tę patową sytuację mianem „cyfrowej zimnej wojny"[54], która od lat paraliżowała nie tylko prace głównych organów ONZ, lecz również ITU.

Reasumując ten wątek, należy stwierdzić, iż Międzynarodowy Związek Telekomunikacyjny stał się w zasadzie jedyną organizacją systemu ONZ, której aktywność na polu cyberbezpieczeństwa doprowadziła do wypracowania wielu niezwykle wartościowych mechanizmów współpracy międzynarodowej. Stało się tak mimo poważnych kontrowersji związanych m.in. z aktualizacją ITR czy zarzutami o sprzyjanie polityce rosyjskiej. Od drugiej połowy pierwszej dekady XXI wieku ITU skupił się głównie na przeciwdziałaniu takim zagrożeniom, jak cyberprzestępczość czy cyberterroryzm, rozwijając szereg interesujących instrumentów praktycznej kooperacji krajów członkowskich w cyberprzestrzeni, czego symbolem stał się przede wszystkim ITU-IMPACT. Nie świadczyło to o braku zainteresowania problematyką rywalizacji i konfrontacji państw w tym środowisku, ponieważ przedstawiciele ITU, w tym przede wszystkim sekretarz generalny, wielokrotnie nawiązywali do tych zagadnień, formułując szereg interesujących propozycji. Ze względu na omówioną wyżej różnicę zdań między dwoma blokami realizacja tych propozycji okazała się jednak niemożliwa. W związku z tym ITU odnotowała największe sukcesy w obszarach, gdzie spory były zdecydowanie mniejsze.

5.3. Polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego[55]

Oprócz omówionych wyżej przedsięwzięć mających z reguły charakter uniwersalny w środowisku międzynarodowym podejmowane są coraz częściej działania o zasięgu regionalnym. Z pewnością jednym z najciekawszych przykładów tych tendencji jest Pakt Północnoatlantycki, który problematykę cyberbezpie-

[54] *A digital cold war?* „The Economist" 14.12.2014: www.economist.com/blogs/babbage/2012/12/internet-regulation; dostęp: 10.03.2014.

[55] Rozdział został opracowany na podstawie artykułu: Lakomy, 2013b.

czeństwa postrzega przez pryzmat pełnionych przez siebie funkcji sojuszu wojskowego. Warto szerzej omówić podstawowe cechy i kierunki polityki NATO w tym zakresie.

Na wstępie należy zaznaczyć, że Organizacja Paktu Północnoatlantyckiego zainteresowała się zagrożeniami teleinformatycznymi stosunkowo późno, dopiero pod koniec lat 90. XX wieku. Było to o tyle zastanawiające, że już zdecydowanie wcześniej pojawiały się, m.in. w USA, głosy wskazujące na niekorzystne reperkusje rozwoju cyberprzestrzeni dla bezpieczeństwa narodowego i międzynarodowego, także w wymiarze *stricte* militarnym. Niemniej problem ten został zauważony przez Sojusz Północnoatlantycki dopiero w wyniku interwencji w Kosowie, która rozpoczęła się w marcu 1999 roku. W związku z masowymi bombardowaniami Serbii przez siły powietrzne państw NATO doszło wówczas do zdecydowanej reakcji tamtejszych haktywistów patriotycznych, którzy podjęli szeroko zakrojoną jak na tamte czasy kampanię cyberataków. Odwołując się do metody DDoS, wzięto na cel stronę internetową Paktu, w wyniku czego przez kilka dni stała się ona niedostępna dla internautów. Po drugie zaczęto blokować sojuszniczy serwer poczty elektronicznej, wysyłając na niego ok. 2000 wiadomości dziennie. Serbom udało się również zainfekować sieć e-mail NATO znanym wówczas złośliwym programem *Happy 1999*. Operację tę można było oceniać z dwóch perspektyw. Z jednej strony ograniczyła się ona do stosunkowo niegroźnych incydentów teleinformatycznych, ponieważ haktywistom nie udało się uzyskać dostępu do wewnętrznych sieci wojskowych, z drugiej jednak strony konsekwencje nawet tych prostych cyberataków były dla organizacji i tak nad wyraz bolesne, gdyż ujawniono jej wrażliwość na zastosowanie tego typu instrumentów. Ponadto utrudniło to prowadzoną przez Sojusz Północnoatlantycki politykę informacyjną w trakcie interwencji. John Pike z Amerykańskiej Federacji Naukowców (Federation of American Scientists) posunął się wręcz do stwierdzenia, iż był to modelowy przykład niezbyt kosztownego cyberataku o dużej wartości[56].

Incydenty wymusiły na Kwaterze Głównej pierwsze kroki zmierzające do poprawy stanu zabezpieczeń wykorzystywanej infrastruktury teleinformatycznej, nadal jednak nie traktowano tej sprawy priorytetowo. Dopiero na szczycie praskim w 2002 roku podjęto bardziej zorganizowane działania w tej sprawie. Zdecydowano wówczas o powołaniu Zdolności Reagowania na Incydenty Komputerowe (Computer Incident Response Capability — CIRC). Została ona zlokalizowana w dwóch miejscach: w Brukseli, gdzie znajdowało się centrum koordynacyjne, oraz w Mons, gdzie rozmieszczono centrum techniczne. Za główne zadanie CIRC uznano ochronę sieci komputerowych NATO, w tym w szczególności zwalczanie wirusów komputerowych oraz przeciwdziałanie włamaniom (Myrli, 09 E BIS).

[56] D. Verton: *Serbs launch cyberattack on NATO*. FCW, 04.04.1999: http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx; dostęp: 12.03.2014.

Stosunkowo szybko okazało się, że podjęte w Pradze decyzje były dalece niewystarczające, obejmowały bowiem wyłącznie ochronę sieci samej organizacji, pomijając szerokie spektrum zagadnień związanych z bezpieczeństwem poszczególnych państw członkowskich. Nieprzygotowanie NATO stało się w pełni widoczne w kwietniu i maju 2007 roku[57]. Jak wspomniano wcześniej, masowe cyberataki przeciwko Estonii stanowiły jeden z najdonioślejszych przykładów rosnącej skali zagrożeń bezpieczeństwa teleinformatycznego. Władze w Tallinie w odpowiedzi na owe wydarzenia wezwały Sojusz Północnoatlantycki do zajęcia się tą sprawą, tym bardziej, iż wcześniej nie wykazywał on większego zainteresowania problematyką (Laasme, 2011; Ruus, 2008). Reakcja NATO okazała się jednak dalece niewystarczająca: Kwatera Główna skierowała co prawda do Estonii dwóch specjalistów ds. cyberbezpieczeństwa, nie zdążyli oni jednak odegrać większej roli[58].

Bezsilność w obliczu masowych cyberataków zagrażających infrastrukturze krytycznej państwa członkowskiego uświadomiła władzom Sojuszu zasadnicze nieprzystosowanie organizacji do skutecznego wypełniania swoich podstawowych funkcji na początku XXI wieku. Powstało więc pytanie, w jaki sposób NATO powinno reagować na poważne włamania do sieci państw członkowskich. Była to sprawa o fundamentalnym znaczeniu, która stawiała pod znakiem zapytania nie tylko dotychczasową praktykę współpracy międzysojuszniczej, ale także podstawy prawne funkcjonowania Paktu. Traktat waszyngtoński podpisany 4 kwietnia 1949 roku został opracowany w warunkach zimnowojennych, jego zapisy były zatem dostosowane do warunków panujących ówcześnie w środowisku bezpieczeństwa. Świadczyły o tym zapisy dwóch podstawowych dla tego dokumentu artykułów. W artykule 5. stwierdzono:

> Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez artykuł 51. *Karty Narodów Zjednoczonych*, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego.

Z kolei w artykule 6. zdefiniowano, że w kategorii zbrojnej napaści zawiera się atak „na siły zbrojne, okręty lub samoloty którejkolwiek ze Stron znajdujące się na tych terytoriach lub nad nimi" (*Traktat północnoatlantycki*, 1949).

[57] Warto zauważyć, iż już na szczycie w Rydze w 2006 roku wspomniano o wzmocnieniu odporności sieci natowskich przed cyberatakami. Zob. Tikk, 2011a: 44.

[58] B. Toth: *Estonia under cyber attack*. Hun-CERT, s. 5: www.cert.hu/sites/default/files/Estonia_attack2.pdf; dostęp: 14.03.2014.

Powyższe zapisy, jak widać, nie brały pod uwagę wystąpienia nieznanych wówczas, z pozoru nieinwazyjnych sposobów ataku na siły zbrojne bądź infrastrukturę krytyczną. W kontekście wydarzeń w Estonii niezaktualizowane regulacje traktatu waszyngtońskiego wiązały się więc z szeregiem poważnych problemów. Przede wszystkim, jak pisał Martin C. Libicki (2013: 61), uznanie przez Pakt cyberbezpieczeństwa za część kolektywnej obrony wiązało się z wątpliwością, czy będzie to w stanie zredukować potencjalne szkody bez jednoczesnego tworzenia nowych wyzwań dla całego Sojuszu. Po drugie, mając na uwadze omówione już wcześniej cechy zagrożeń teleinformatycznych, traktat waszyngtoński wydawał się wykluczać z kategorii napaści zbrojnej niemal wszystkie ataki komputerowe. Jak wiadomo, z reguły nie stwarzają one fizycznych zniszczeń, które można by jednoznacznie uznać za „zbrojną napaść" (Ellis, 2001: 3). Po trzecie nie muszą one brać na cel elementów składających się na siły zbrojne państw członkowskich, zdecydowanie poważniejsze konsekwencje dla bezpieczeństwa narodowego miałoby natomiast zaatakowanie elementów infrastruktury krytycznej. Po czwarte w przestrzeni teleinformatycznej stosowanie podstawowych i dość oczywistych kategorii integralności terytorialnej, suwerenności państwowej lub tradycyjnie rozumianych granic jest utrudnione[59]. Po piąte traktat waszyngtoński pomijał szereg problemów związanych z identyfikacją sprawców, co jest rzeczą naturalną dla środowiska teleinformatycznego. Z punktu widzenia funkcjonowania NATO jest to sprawa o zasadniczym znaczeniu, ponieważ incydenty na tle przestępczym nie powinny z natury wywoływać reakcji sojuszu wojskowego. Po szóste nie wzięto także pod uwagę kwestii, w jaki sposób należałoby oceniać cyberataki pod względem ich liczby, trzeba bowiem pamiętać, iż mają one współcześnie charakter coraz bardziej masowy. Można tu przytoczyć przykład amerykańskiej agencji NNSA (National Nuclear Security Administration), która w 2012 roku była atakowana nawet 10 milionów razy dziennie[60]. Powstaje zatem pytanie, w jaki sposób z tego bezliku wyodrębnić te, które wiążą się z określonymi konsekwencjami prawno-politycznymi, tym bardziej, iż analiza nawet pojedynczej sytuacji może trwać tygodnie bądź

[59] Warto jednak zaznaczyć, iż nie ma pełnej zgody badaczy w tej sprawie. Część wskazuje, że są to terminy nadal przydatne do stosowania w cyberprzestrzeni. Z reguły głosy te pomijają jednak szereg wątpliwości związanych m.in. z trudną do jednoznacznej oceny technologią *cloud computingu*. Zob. np. Heintschel von Heinegg, 2013: 123—156; Wu, 1997: 648—665; Ellis, 2001: 3; F. Hare: *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security*? CCD COE: www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf; dostęp: 12.03.2014; L. Wang, G. von Laszewski: *Scientific Cloud Computing: Early Definition and Experience*. Rochester Institute of Technology, 26.10.2008: http://cyberaide.googlecode.com/svn/trunk/papers/08-cloud/vonLaszewski-08-cloud.pdf; dostęp: 12.03.2014.

[60] J. Koebler: *U.S. Nukes Face Up to 10 Milion Cyber Attacks Daily*. USA News, 20.03.2012: www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily; dostęp: 12.03.2014.

miesiące. W przypadku miliardów incydentów teleinformatycznych jest to niezwykle trudne, a czasami wręcz niewykonalne zadanie.

Wszystkie te wątpliwości stały się niezwykle aktualne właśnie w 2007 roku za sprawą wydarzeń w Estonii. Traktat waszyngtoński będący fundamentem funkcjonowania Paktu Północnoatlantyckiego nie przewidywał tutaj, jak widać, możliwości reakcji na ataki teleinformatyczne wymierzone w państwa członkowskie. Nie było to z pewnością korzystne rozwiązanie, co sprawiło, iż Sojusz energicznie zajął się tą problematyką. Prace w tej dziedzinie były prowadzone dwutorowo: zaczęto się zastanawiać, w jaki sposób reagować na tego typu cyberzagrożenia w sensie politycznym i prawnym, podjęto także działania, które miały podnieść praktyczną gotowość NATO do zwalczania włamań do sieci komputerowych.

Jeśli chodzi o wymiar koncepcyjny i polityczny, to należy stwierdzić, iż już w 2007 roku doszło do pierwszych przewartościowań w polityce natowskiej. Problem ataków wymierzonych w Estonię omówiono na szczytach Paktu w czerwcu oraz październiku 2007 roku. Na pierwszym z nich ministrowie obrony zgodzili się co do potrzeby przyjęcia ramowego dokumentu, który stanowiłby odpowiedź na narastające zagrożenia dla cyberbezpieczeństwa NATO[61], na drugim natomiast, w Nordwijk, zapoznano się z raportem, który ocenił stan przygotowania Sojuszu do obrony przez wyzwaniami pojawiającymi się online. Zawarto tam szereg rekomendacji, które miały być zrealizowane w kolejnych latach (Myrli). W wyniku tych spotkań w styczniu 2008 roku opracowano tajny dokument na temat „polityki cyberobrony" organizacji (*NATO on Cyber Defence Policy*). Przywódcy państw członkowskich Sojuszu zatwierdzili go ostatecznie w kwietniu tego roku na szczycie w Bukareszcie. Zwiększone zainteresowanie tematyką cyberbezpieczeństwa znalazło swój wyraz w dokumencie końcowym tej konferencji, w którym zadeklarowano, iż Sojusz będzie dążył do wzmocnienia ochrony systemów informacyjnych przed cyberatakami, a ponadto, podkreślając wagę przyjętego dokumentu na temat cyberbezpieczeństwa, zobowiązano się do stworzenia nowych organów odpowiedzialnych za realizację jego założeń. Na koniec opowiedziano się za wzmocnieniem współpracy między instytucjami NATO a poszczególnymi państwami członkowskimi, co słusznie zinterpretowano jako próbę odpowiedzi na incydenty w Estonii (*Bucharest Summit Declaration*, 2008; Myrli).

Omówione wyżej ruchy nie zakończyły bynajmniej prac Sojuszu Północnoatlantyckiego na tym obszarze. Kwestie te szerzej przedyskutowano już podczas szczytu NATO w Strasbourgu w 2009 roku. W deklaracji końcowej z 4 kwietnia zawarto stwierdzenia, które świadczyły o tym, iż przyznano priorytetowy sta-

[61] J. McGee: *NATO and Cyber Defence: A Brief Overview and Recent Events*. Center for Strategic & International Studies, 08.07.2011: https://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events; dostęp: 12.03.2014.

tus bezpieczeństwu teleinformatycznemu. Zadeklarowano, że organizacja będzie kontynuować wysiłki zmierzające do rozwoju swoich zdolności i potencjału w tym zakresie, rozumiejąc skalę zagrożeń wynikających zarówno z aktywności państw, jak i podmiotów pozapaństwowych. Za dotychczasowe sukcesy uznano powołanie szeregu organów zajmujących się cyberbezpieczeństwem (Centrum Doskonalenia Cyberobrony, Organu Zarządzającego Cyberobroną), a także usprawnienie funkcjonowania CIRC. Przyznano ponadto, że „cyberobrona" stanie się integralną częścią ćwiczeń prowadzonych przez Sojusz. Zaakcentowano również potrzebę rozwijania kontaktów z innymi organizacjami międzynarodowymi (*Strasbourg/Kehl Summit Declaration*, 2009).

O rosnącym znaczeniu tych zagadnień świadczyły jednak przede wszystkim decyzje podjęte w Lizbonie w 2010 roku, w nowej koncepcji strategicznej Sojuszu *Active Engagement, Modern Defence* zawarto bowiem kilka niezwykle istotnych stwierdzeń. W punkcie 12. zauważono rosnące zagrożenie wspólnoty euroatlantyckiej cyberatakami wymierzonymi m.in. we wrażliwe elementy infrastruktury krytycznej. Wśród ich źródeł wymieniono nie tylko organizacje przestępcze, ekstremistyczne czy terrorystyczne, ale również obce siły zbrojne oraz agencje wywiadowcze. Świadczyło to o świadomości, iż przestrzeń teleinformatyczna stawała się w coraz większym stopniu polem rywalizacji państw. W związku z tym w punkcie 19. zadeklarowano, iż Sojusz będzie podnosił swoje zdolności do zapobiegania i wykrywania ataków komputerowych oraz do obrony przed nimi, jak również do sprawnej likwidacji poczynionych przez nie szkód. W tym celu NATO miało wzmacniać i koordynować narodowe potencjały „cyberobrony", jak również zapewnić wszystkim strukturom organizacji ochronę teleinformatyczną. Stwierdzono ponadto, iż sojusznicze systemy wykrywania zagrożeń w cyberprzestrzeni i reagowania na nie zostaną zintegrowane z systemami poszczególnych krajów członkowskich (*Active Engagement, Modern Defence*, 2010). Spostrzeżenia te powtórzono i poszerzono w deklaracji końcowej szczytu w Lizbonie. W punkcie 2. zadeklarowano, iż Sojusz będzie rozwijał swoje zdolności do „cyberobrony". W punkcie 24. wśród zagrożeń transnarodowych wymieniono właśnie te, które pojawiają się w przestrzeni teleinformatycznej. Przeciwdziałanie im w strategii NATO miało być oparte m.in. na pogłębionym partnerstwie z innymi podmiotami stosunków międzynarodowych. W punkcie 40. podkreślono, że wymiar cyberprzestrzenny zostanie wzięty pod uwagę w działaniach Sojuszu, tak aby był on zdolny do wykrywania, oceny i prewencji ataków komputerowych wymierzonych w systemy o krytycznym znaczeniu dla organizacji oraz do obrony przed nimi. W tym celu zadeklarowano, iż NATO będzie działać na rzecz osiągnięcia przez CIRC pełnej gotowości operacyjnej do 2012 roku, a także objęcia wszystkich jego organów ochroną teleinformatyczną. Złożono także obietnicę pogłębiania współpracy z Organizacją Narodów Zjednoczonych oraz Unią Europejską. O przeciwdziałaniu cyberatakom wspomniano również w punkcie 45 (*Lisbon Summit Declaration*, 2010).

Porównując te zapisy z wcześniejszymi deklaracjami politycznymi Sojuszu, należy stwierdzić, iż w 2010 roku dokonano pewnego przełomu, po raz pierwszy bowiem na taką skalę podkreślono wolę kooperacji w dziedzinie bezpieczeństwa teleinformatycznego, trafnie identyfikując podstawowe zagrożenia, ich źródła, a także środki przeciwdziałania im.

Prace koncepcyjne były kontynuowane w 2011 roku: 8 czerwca ministrowie obrony państw członkowskich przyjęli zaktualizowaną wersję strategii cyberobronnej — *NATO Policy on Cyber Defence*, w październiku tego roku uzgodnili natomiast podstawowe pryncypia planu działań (*Action Plan*)[62]. W tym kontekście można przywołać słowa Jasona Healeya oraz Leenderta van Bochovena, którzy wskazali na następujące cechy nowego podejścia:

- świadomość, że cyberobrona jest potrzebna, aby NATO było w stanie pełnić swoje podstawowe funkcje zbiorowej obrony oraz zarządzania kryzysowego,
- przeciwdziałanie, elastyczność oraz obrona krytycznych dla NATO i jego członków systemów teleinformatycznych (*cyber assets*),
- implementacja skutecznych zdolności cyberobronnych oraz scentralizowanej ochrony sieci NATO,
- zdefiniowanie podstawowych wymagań w zakresie cyberobrony tych narodowych sieci, które są krytyczne dla wypełniania przez organizację swoich zadań,
- wsparcie państw członkowskich w pracach na rzecz uzyskania podstawowych zdolności cyberobronnych w celu zminimalizowania zagrożenia dla narodowych infrastruktur krytycznych,
- współpraca z innymi podmiotami, takimi jak organizacje międzynarodowe, sektor prywatny czy środowisko naukowe (Healey, van Bochoven, 2012: 3).

W maju 2012 roku na spotkaniu szefów państw i rządów w Chicago potwierdzono te priorytety. W dokumencie pod tytułem *Deterrence and Defence Posture Review* w punkcie 4. zauważono, iż cyberzagrożenia, obok problemów energetycznych i ekologicznych, będą determinować przyszłe środowisko bezpieczeństwa Sojuszu. W punkcie 14. uznano, iż konwencjonalne siły sojusznicze muszą być przygotowane do współudziału w zwalczaniu zagrożeń teleinformatycznych. W punkcie 18. natomiast po raz kolejny zauważono potrzebę rozwijania zdolności do obrony sieci komputerowych (*Deterrence and Defence*, 2012). W deklaracji poświęconej potencjałowi obronnemu (*Summit Declaration on Defence Capabilities: Toward NATO Forces 2020*) stwierdzono znaczny postęp natowskich zdolności do odpierania cyberataków (*Summit Declaration*, 2012). W deklaracji końcowej szczytu zagadnieniom bezpieczeństwa teleinformatycznego poświęcono punkt 49. w którym powtórzono, iż w związku ze wzrastającym zagrożeniem incydentami komputerowymi NCIRC osiągnie gotowość operacyjną do końca

[62] *NATO and Cyber Defence*. NATO.int: www.nato.int/cps/en/natolive/topics_78170.htm?; dostęp: 14.03.2014.

2012 roku. Podkreślono ponadto, że poczynione wysiłki zmierzają do objęcia zcentralizowaną ochroną wszystkich struktur wchodzących w skład Organizacji Paktu Północnoatlantyckiego. Po raz kolejny zadeklarowano również chęć współpracy z innymi organizacjami międzynarodowymi, przy czym tym razem poza UE oraz ONZ wymieniono inne: Radę Europy oraz Organizację Bezpieczeństwa i Współpracy w Europie (*Chicago Summit Declaration*, 2012).

Istotne decyzje Sojusz podjął w 2013 roku: 4 czerwca odbyło się pierwsze w historii spotkanie ministrów obrony państw członkowskich poświęcone wyłącznie kwestiom cyberbezpieczeństwa. Warto przytoczyć kilka najważniejszych ustaleń z tego spotkania. Przede wszystkim należy wspomnieć o ważnym wystąpieniu sekretarza generalnego NATO Andersa Fogha Rasmussena, który na konferencji prasowej przyznał, iż cyberataki wymierzone w Sojusz mogą mieć „dewastujące konsekwencje". Przytoczył też dane, według których sieci Paktu zostały w 2012 roku poważnie zaatakowane ok. 2500 razy, choć żadnemu z nich nie udało się znaleźć luk w zabezpieczeniach. Podkreślił także, iż znaczenie bezpieczeństwa teleinformatycznego rośnie, wszyscy sojusznicy są bowiem ze sobą połączeni na wiele sposobów, a zatem włamanie do sieci jednego może oznaczać uzyskanie dostępu do intranetu całej organizacji. Stwierdził także, iż „cyberataki nie zatrzymują się na granicach, [więc — M.L.] nasza obrona również nie powinna". W związku z tym na spotkaniu ministrów obrony zdecydowano m.in. o powołaniu Zespołów Szybkiego Reagowania (Rapid Reaction Teams), które miały osiągnąć gotowość operacyjną do końca 2013 roku. Ruch ten, jak określił to Anders Fogh Rasmussen, oznaczał wejście dopiero w pierwszą fazę nowej polityki cyberbezpieczeństwa NATO. Druga miała polegać na dokonaniu przeglądu sposobów reakcji organizacji na włamania do sieci państw członkowskich[63]. W październiku 2013 roku na kolejnym spotkaniu ministrów obrony Sojuszu potwierdzono natomiast obrany w czerwcu kierunek prac nad rozwojem zdolności do cyberobrony[64].

Omówionym wyżej działaniom o charakterze koncepcyjnym bądź politycznym towarzyszyły wielokierunkowe przedsięwzięcia zmierzające do wypracowania przez Sojusz praktycznych mechanizmów reagowania na incydenty teleinformatyczne. Warto scharakteryzować najważniejsze z nich. Na wstępie można zauważyć, że w wyniku decyzji podjętych jeszcze w 2007 roku już w rok później powołano dwie niezwykle ważne instytucje. Pierwszą było utworzone w maju 2008 roku Centrum Doskonalenia Cyberobrony (Cooperative Cyber Defence Centre of Excellence — CCD COE), które zlokalizowano

[63] *Press Conference by NATO Secretary General Anders Fogh Rasmussen following the NATO Defence Ministers meeting on 4 June 2013*. NATO, 04.06.2013: www.nato.int/cps/en/natolive/opinions_101151.htm; dostęp: 15.03.2014.

[64] *Opening remarks by NATO Secretary General Anders Fogh Rasmussen at the North Atlantic Council Meeting in Defence Ministers sessions*. NATO, 22.10.2013: www.nato.int/cps/en/natolive/opinions_104256.htm; dostęp: 15.03.2014.

w Tallinie. Zostało ono utworzone przez Sojusznicze Dowództwo Transformacji (Allied Command Transformation — ACT) wraz z 7 państwami członkowskimi: Estonią, Niemcami, Włochami, Łotwą, Litwą, Słowacją oraz Hiszpanią. Do głównych funkcji nowo powołanej struktury zaliczono podnoszenie zdolności do działań w cyberprzestrzeni, jak również współpracy oraz wymiany informacji zarówno w samym NATO, jak i między Sojuszem a innymi partnerami zewnętrznymi. Jak stwierdzono na stronie internetowej tego organu, Centrum miało w założeniu stać się głównym źródłem ekspertyz na temat „kooperatywnej cyberobrony", CCD COE powinno więc prowadzić prace koncepcyjne, szkoleniowe i badawcze, które stale podnosiłyby jakość polityki cyberbezpieczeństwa Paktu Północnoatlantyckiego[65]. Efekty funkcjonowania Centrum można oceniać z dwóch perspektyw. Z jednej strony warto zauważyć, iż zainteresowanie aktywnością w jego ramach okazało się stosunkowo niewielkie. W kolejnych latach liczba państw partycypujących w CCD COE wzrosła tylko nieznacznie. Świadczył o tym fakt, iż dopiero w 2011 roku dołączyły do niego Stany Zjednoczone oraz Polska[66]. Oznaczało to, że jego możliwości działania były mimo wszystko dość ograniczone. Z drugiej jednak strony bez względu na te problemy Centrum udało się osiągnąć spektakularne sukcesy. Dzięki temu stało się jednym z czołowych światowych ośrodków zajmujących się badaniami nad zagrożeniami dla ICT, ponieważ od momentu powstania organizowało nie tylko specjalistyczne kursy oraz konferencje, ale również przygotowywało wartościowe opracowania naukowe. W zasadzie największy rozgłos uzyskał opublikowany pod koniec 2012 roku podręcznik *Tallinn Manual on the International Law Applicable to Cyber Warfare*[67]. W związku z jego globalnym sukcesem CCD COE rozpoczęło projekt *Tallin 2.0*, którego celem stała się rozbudowa podręcznika o kolejne nie-

[65] *Mission and Vision*. CCD COE: www.ccdcoe.org/11.html; dostęp: 12.03.2014.

[66] *Centre Welcomes Two New Members*. CCD COE: www.ccdcoe.org/295.html; dostęp: 12.03.2014.

[67] W 2009 roku Centrum Doskonalenia Cyberobrony NATO zleciło grupie kilkudziesięciu uznanych międzynarodowych ekspertów pracujących pod kierunkiem Michaela N. Schmitta przygotowanie podręcznika, który omówiłby podstawowe zasady prawa międzynarodowego regulującego zjawisko cyberwojny. Co prawda tego typu próby były podejmowane wcześniej już wielokrotnie, nigdy jednak na taką skalę oraz przez tak utytułowany i doświadczony zespół. W efekcie powstało dzieło, w którym zaproponowano szereg niezwykle interesujących rozwiązań dotyczących interpretacji incydentów teleinformatycznych z perspektywy obowiązujących regulacji prawa międzynarodowego. W sumie scharakteryzowano w nim 95 zasad dotyczących m.in. takich kwestii, jak suwerenność, jurysdykcja, odpowiedzialność państwa czy użycie siły w cyberprzestrzeni, zakres obowiązywania prawa wojny w sieci, środki walki, cyberszpiegostwo czy status i ochrona nieletnich. Warto dodać, iż publikacja ta jest niezwykle wartościowa nie tylko z punktu widzenia nauk prawnych, lecz również nauk politycznych i nauk o bezpieczeństwie, zawiera bowiem wiele cennych spostrzeżeń i propozycji dotyczących rozumienia trudnych bądź kontrowersyjnych terminów (o czym zresztą wspominano wcześniej), takich jak *cyberoperacja*, *cyberatak*, *system komputerowy*, *haktywista*, *haker*, *złośliwe oprogramowanie* czy *wirus*. Zob. Schmitt, ed., 2013.

zbędne elementy. Warto dodać, iż była to prawdopodobnie najgłośniejsza oraz najbardziej wartościowa praca naukowa, w której zawarto propozycje mogące stać się punktem wyjścia dla przedsięwzięć podejmowanych w ramach Organizacji Narodów Zjednoczonych. Wśród innych przejawów aktywności Centrum można wyróżnić także organizację ćwiczeń i szkoleń (np. *Baltic Cyber Shield, Locked Shield*)[68]. Co jednak najważniejsze, CCD COE stało się symbolicznym wyrazem energicznej reakcji Sojuszu Północnoatlantyckiego na ataki komputerowe na Estonię z kwietnia i maja 2007 roku.

Drugą instytucją powołaną w tym samym czasie był Organ Zarządzający Cyberobroną (Cyber Defence Management Authority — CDMA), który rozpoczął działalność w kwietniu 2008 roku. W przeciwieństwie do CCD COE uzyskał on dwie interesujące kompetencje w wymiarze *stricte* praktycznym. Po pierwsze miał on koordynować reakcję na ataki teleinformatyczne, jeśli zostałby o to poproszony przez państwa członkowskie, po drugie natomiast zlecono mu tworzenie podstawowych standardów i procedur w dziedzinie cyberbezpieczeństwa, które byłyby przedkładane zarówno agencjom rządowym, jak i całej organizacji. Posiadając odpowiednie zdolności techniczne, stał się pierwszą strukturą natowską, która mogła udzielić wsparcia w razie poważnego cyberataku zagrażającego bezpieczeństwu narodowemu któregoś z członków. Warto dodać, iż od początku Organ Zarządzający Cyberobroną wykazywał wysoką aktywność, czego przejawem było z jednej strony zorganizowanie wspólnych ćwiczeń państw członkowskich w cyberprzestrzeni, a z drugiej wysłanie swojego przedstawiciela do Gruzji w trakcie wojny z Rosją w sierpniu 2008 roku[69].

Kolejne istotne przedsięwzięcia w wymiarze praktycznym rozpoczęto w lutym 2012 roku, kiedy przeznaczono 58 mln euro na osiągnięcie przez NCIRC pełnej zdolności operacyjnej do jesieni 2013 roku. W tym okresie ustanowiono również Komórkę Świadomości Cyberzagrożeń (Cyber Threat Awareness Cell), której głównym zadaniem było wspomaganie wymiany danych wywiadowczych, a także podnoszenie „świadomości sytuacyjnej". W kwietniu 2012 roku rozpoczęto natomiast integrację sojuszniczych zdolności cyberobronnych z Procesem Planowania Obronnego NATO (NATO Defence Planning Process)[70]. Następnie 1 lipca 2012 roku powołano Agencję Komunikacji

[68] *Cyber Defence Exercises*. CCD COE: www.ccdcoe.org/353.html; dostęp: 14.03.2014.

[69] W późniejszym czasie CDMA zaczęła funkcjonować jako Komitet Zarządzający Cyberobroną (Cyber Defence Management Board — CDMB). Zob. *NATO sets up Cyber Defence Management Authority*. „Computer Weekly" 04.04.2008: www.computerweekly.com/news/2240085580/Natosets-up-Cyber-Defence-Management-Authority-in-Brussels; dostęp: 14.03.2014; *NATO Agrees to Create Cyber Defence Management Authority*. Internet Business Law Services: www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2054; dostęp: 14.03.2014; Myrli; *Defending the networks. The NATO Policy on Cyber Defence*. NATO: www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf; dostęp: 14.03.2014.

[70] *NATO and Cyber Defence*. NATO.int: www.nato.int/cps/en/natolive/topics_78170.htm?; dostęp: 14.03.2014.

i Informacji (NATO Communications and Information Agency — NCI), która powstała z połączenia kilku struktur: NC3A, NACMA, NCSA i ALTBMD. Do jej głównych funkcji zaliczono świadczenie usług w zakresie dowodzenia, kontroli, komunikacji, komputerów, wywiadu oraz obserwacji i rozpoznania (C4ISR). W praktyce NCI posiadła kompetencje w wielu dziedzinach, począwszy od prac badawczo-rozwojowych aż po prowadzenie szkoleń oraz misji. Należy podkreślić, iż obrona teleinformatyczna stała się jednym z podstawowych aspektów funkcjonowania Agencji. W ramach pełnienia tych zadań NCI wsparła m.in. Międzynarodowy Projekt Rozwoju Zdolności Cyberobrony (Multinational Cyber Defence Capabilities Development Project), który został rozpoczęty w marcu 2013 roku przez Kanadę, Danię, Holandię, Norwegię i Rumunię. Jego podstawowym celem było podniesienie potencjału do cyberobrony poprzez intensyfikację współpracy międzynarodowej. W ramach MNCD2 przewidziano m.in. koordynację prac badawczych, wymianę informacji o zagrożeniach teleinformatycznych i sposobach ich zwalczania. Projekt pozostał w pełni otwarty dla innych państw członkowskich NATO[71].

Do końca 2013 roku zrealizowano także koncepcję Zespołów Szybkiego Reagowania (Rapid Reaction Teams), którą wysunięto jeszcze w 2011 roku. Początkowo zakładano, iż miały one składać się z sześciu ekspertów komputerowych zdolnych do pomocy państwom członkowskim w razie ataku teleinformatycznego. Zgodnie z tym założeniem RRT miały być uruchamiane tylko na wniosek rządu i w pełni mu podlegać w trakcie misji, w zasadzie była to więc inicjatywa skierowana do tych krajów, które nie zdążyły jeszcze wypracować własnych zdolności w tej dziedzinie[72]. Projekt ten spotkał się jednak z pewnym oporem, co doprowadziło do opóźnień i modyfikacji samego pomysłu, ponieważ na wspomnianym już spotkaniu ministrów Sojuszu w czerwcu 2013 roku uznano, że RRT będą służyły wyłącznie do ochrony sieci samej organizacji. Nie wykluczono jednak rozszerzenia kompetencji tych grup w przyszłości właśnie o wsparcie udzielane państwom członkowskim (Chamberlain, 2013: 2). Taki ruch był dość zaskakujący, funkcjonowały już bowiem inne organy przeznaczone do ochrony sieci komputerowych NATO. Tymczasem, jak udowodnił *casus* Estonii, poważnym problemem pozostawała pomoc dla zaatakowanych członków. W tym kontekście Anders Fogh Rasmussen sugerował w czerwcu 2013 roku, iż wyjściem z tej sytuacji mogłoby być wykorzystanie potencjału eksperckiego, będącego do dyspozycji poszczególnych rządów. Byłoby to więc powielenie praktyki znanej chociażby z przypadku Turcji, do której przerzucono w 2013 roku amerykańskie baterie rakiet przeciwlotniczych Patriot[73].

[71] *NATO and Cyber Defence…*, op.cit.; *Multinational Cyber Defence Capability Development*, 2013.

[72] *NATO Rapid Reaction Team to fight cyber attack*. North Atlantic Treaty Organization News, 13.03.2012: www.nato.int/cps/en/natolive/news_85161.htm; dostęp: 14.03.2014.

[73] *Press Conference by NATO Secretary General…*, op.cit.

Można także wspomnieć o kilku innych organach Sojuszu Północnoatlantyckiego, które zyskały pewne znaczenie dla jego polityki cyberbezpieczeństwa. Za Jasonem Healeyem oraz Leendertem van Bochovenem można tu wymienić następujące struktury:

1. Radę Północnoatlantycką (North Atlantic Council), która jest głównym organem wyznaczającym kierunki rozwoju oraz priorytety polityki bezpieczeństwa teleinformatycznego NATO.
2. Komitet Planowania i Polityki Obrony (Defense Policy and Planning Committee), który konkretyzuje ogólne wskazówki i decyzje podjęte przez NAC.
3. Sojusznicze Dowództwo Transformacji (Allied Command Transformation), które nadzoruje Centrum Doskonalenia Cyberobrony (CCD COE) w Tallinie oraz odpowiada za wypracowanie koncepcji zwalczania zagrożeń teleinformatycznych.
4. Wydział Wschodzących Wyzwań dla Bezpieczeństwa Kwatery Głównej (Headquarters Emerging Security Challenges Division) odpowiedzialny za zwalczanie niekonwencjonalnych wyzwań dla bezpieczeństwa NATO, w tym m.in. cyberataków.
5. Agencję C3 (C3 Agency) odpowiedzialną za rozpoznawanie potrzeb operacyjnych oraz wdrażanie nowych rozwiązań (Healey, van Bochoven, 2012: 3).

Na tej podstawie można stwierdzić, iż Sojusz Północnoatlantycki wypracował do końca 2013 roku politykę cyberbezpieczeństwa ufundowaną na kilku założeniach. Należy do nich zaliczyć ochronę własnych sieci i systemów teleinformatycznych, zintegrowanie polityki NATO z wysiłkami państw członkowskich w tej dziedzinie, formułowanie minimalnych wymogów dla narodowych systemów teleinformatycznych, podłączonych do systemów sojuszniczych, pomoc zaatakowanym w cyberprzestrzeni członkom organizacji, rozwój współpracy z innymi organizacjami międzynarodowymi, środowiskiem naukowym oraz sektorem prywatnym, prowadzenie prac badawczych, a także prowadzenie ćwiczeń i szkoleń. Należy dodać, iż realizacja tych priorytetów została oparta na trzech fundamentalnych wartościach: prewencji, zwiększaniu odporności na cyberataki oraz unikaniu dublowania kompetencji istniejących już instytucji i organów[74].

Ukoronowaniem wszystkich tych zabiegów stała się decyzja podjęta w czerwcu 2014 roku o zaktualizowaniu przez ministrów obrony państw członkowskich dotychczasowej polityki cyberbezpieczeństwa Sojuszu Północnoatlantyckiego. Od tej pory uznano, iż cyberobrona wchodzi w skład podstawowych funkcji NATO dotyczących zbiorowej obrony. Innymi słowy stwierdzono, iż mechanizm artykułu 5. traktatu waszyngtońskiego może zostać wykorzystany w razie wystąpienia poważnych ataków teleinformatycznych. Nie określono jed-

[74] *NATO and Cyber Defence*…, op.cit., dostęp: 15.03.2014; *Defending the networks*, 2011.

nak dokładnie, w jakich warunkach może zostać użyty, wychodząc z założenia, iż sojusznicy będą decydować w każdym z przypadków z osobna, bazując na zaobserwowanych zniszczeniach oraz motywacjach sprawców (*malicious intention*). Ponadto potwierdzono, iż według Paktu działania w cyberprzestrzeni są regulowane przez prawo międzynarodowe. Zdecydowano także o intensyfikacji współpracy na innych polach, w tym np. kooperacji przemysłów czy wymiany informacji i doświadczeń[75]. Była to decyzja bez precedensu, która stanowiła symboliczne zwieńczenie wieloletnich prac nad cyberbezpieczeństwem NATO. Jednocześnie była reakcją na omówione wyżej wątpliwości związane z efektywnością reagowania na incydenty teleinformatyczne w krajach członkowskich.

Reasumując, można zauważyć, iż polityka cyberbezpieczeństwa NATO od początku XXI wieku uległa poważnej ewolucji. Początkowo Sojusz Północnoatlantycki nie dostrzegał narastającej skali zagrożeń teleinformatycznych, co doprowadziło do obnażenia jego słabości w 2007 roku. Niemniej prawidłowo oceniając konsekwencje zaniedbań w tej sprawie, jeszcze w tym samym roku podjęto wielokierunkowe prace mające przygotować Pakt do zwalczania nowych wyzwań. Z jednej strony ich celem było wykształcenie odpowiednich rozwiązań politycznych, które miały uodpornić Sojusz na kolejne tego typu kryzysy. Pełna ich ocena nie jest niestety możliwa, ponieważ część dokumentów pozostała niejawna. Opublikowane materiały oraz deklaracje z kolejnych szczytów świadczą jednak o tym, iż przyjęto w miarę racjonalną i elastyczną strategię działania. Nie tylko skupiono się na budowie praktycznych zdolności obrony przed włamaniami, ale także wyrażono chęć nawiązania kontaktów z innymi podmiotami, zarówno z organizacjami międzynarodowymi (ONZ, UE, Rada Europy, OBWE), jak i z poszczególnymi państwami. W odróżnieniu np. od ONZ czy ITU bardzo wyraźnie podkreślano, że cyberprzestrzeń zaczęła być postrzegana jako nowa domena rywalizacji rządów oraz kolejny teatr nowoczesnych konfliktów zbrojnych. Symbolem tej świadomości stała się przełomowa decyzja z czerwca 2014 roku o uwzględnieniu mechanizmu artykułu 5. traktatu waszyngtońskiego w reagowaniu na incydenty teleinformatyczne. Na pozytywną ocenę zasługuje także stosunkowo szybkie stworzenie całego systemu wzajemnie wspierających się organów w tej dziedzinie. Szczególną uwagę, poza rozbudową NCIRC i stworzeniem CDMA, przykuwał projekt Centrum Doskonalenia Cyberobrony — instytucji, która przyczyniła się w znacznym stopniu do lepszego zrozumienia specyfiki cyberzagrożeń na całym świecie.

Z drugiej jednak strony należy podkreślić, iż Pakt Północnoatlantycki, wypracowując pewne podstawowe rozwiązania koncepcyjne oraz praktyczne, pominął kilka istotnych zagadnień. Po pierwsze mimo aktualizacji polityki

[75] S. Ranger: *NATO Updates Policy: Offers Members Article 5 Protection Against Cyber Attacks*. Atlantic Council, 30.06.2014: www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks; dostęp: 13.08.2014; *NATO and Cyber Defence*…, op.cit., dostęp: 13.08.2014.

cyberobronnej Sojuszu w czerwcu 2014 roku nie zdecydowano się na precyzyjne omówienie tego, jak należy w praktyce reagować na incydenty teleinformatyczne. Tym samym w wypadku ewentualnej cyberwojny udzielenie pomocy zaatakowanemu państwu członkowskiemu wynikałoby wyłącznie z woli politycznej. Taka sytuacja może więc osłabiać solidarność sojuszniczą w tej dziedzinie. Po drugie w ciągu 7 lat nie udało się wypracować jasnych rozwiązań dotyczących tego, w jaki sposób NATO mogłoby udzielić bezpośredniej, praktycznej pomocy zaatakowanym w cyberprzestrzeni. Świadczyły o tym wypowiedzi Andersa Fogha Rasmussena z 2013 roku *a propos* użycia Zespołów Szybkiego Reagowania. Po trzecie nie podjęto również jawnej decyzji, która wskazywałaby na wolę wypracowania i ewentualnego użycia przez organizację ofensywnych zdolności w cyberprzestrzeni. Jak stwierdziła w tym kontekście Joanna Świątkowska z Instytutu Kościuszki, „skuteczna obrona to fundament wszelkich działań, jednak możliwość dokonania ataku na potencjalnego rywala w niedalekiej przyszłości stanie się koniecznością”[76]. W ciekawy sposób do tych zagadnień odniósł się również John B. Sheldon, który zauważył, że koordynacja prawie 30 standardów, procedur, strategii i doktryn jest na tyle trudna, iż taki ruch jest mało prawdopodobny. Ponadto według autora sama natura ofensywnych zdolności teleinformatycznych jest na tyle wrażliwa, iż dzielenie się nimi z sojusznikami mogłoby osłabić ich skuteczność[77].

5.4. Bezpieczeństwo teleinformatyczne w pracach Unii Europejskiej[78]

Kolejnym przykładem narastającej współpracy międzynarodowej w zakresie cyberbezpieczeństwa na poziomie regionalnym jest z pewnością Unia Europejska. Jej zainteresowanie tą problematyką wynikało pierwotnie z kilku przesłanek. Po pierwsze było to naturalne ze względu na fakt, iż składa się ona z wielu państw, które posiadają zaawansowane zdolności w tej dziedzinie (Francja, Niemcy, Wielka Brytania). Po drugie wynikało to pośrednio z rozwoju Wspólnej Polityki Zagranicznej i Bezpieczeństwa, której jednym z kluczowych zadań było identyfikowanie nowych wyzwań i przeciwdziałanie im dla bezpie-

[76] J. Świątkowska: *Rola Polski w budowaniu cyberbezpieczeństwa NATO*. Defence24, 09.01.2014: www.defence24.pl/blog_rola-polski-w-budowaniu-cyberbezpieczenstwa-nato; dostęp: 15.03.2014.

[77] J.B. Sheldon: *NATO and Cyber Defense: Hanging Together or Hanging Separately?* United Nations Institute for Disarmament Research: www.unidir.org/en/Audio/listerAudio/idConference:165; dostęp: 15.03.2014.

[78] Rozdział został opracowany na podstawie artykułu: Lakomy, 2013c.

czeństwa i stabilności Unii, zarówno w wymiarze cywilnym, jak i wojskowym (Latoszek, 2007: 520—557). Funkcje te potwierdzono i poszerzono w traktacie lizbońskim, gdzie znalazły się zapisy o solidarności państw UE w wypadku np. ataku terrorystycznego bądź katastrofy spowodowanej przez człowieka. W artykule 42. TUE stwierdzono ponadto, iż „w przypadku gdy jakiekolwiek państwo członkowskie stanie się ofiarą zbrojnej agresji na jego terytorium, pozostałe państwa członkowskie mają w stosunku do niego obowiązek udzielenia pomocy i wsparcia przy zastosowaniu wszelkich dostępnych im środków, zgodnie z artykułem 51. Karty Narodów Zjednoczonych" (cyt. za: Miszczak, 2008: 250—251). Po trzecie wpływały na to postępy współpracy w ramach dawnego trzeciego filaru, czyli wymiaru sprawiedliwości i spraw wewnętrznych (Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości). Zaktualizowany artykuł 67. TFUE wyznaczył np. podstawowe obszary kooperacji, w tym choćby koordynację działań organów policyjnych, zapobieganie przestępczości lub jej zwalczanie (Grzelak, 2008: 276). Po czwarte podobnie jak Sojusz Północnoatlantycki Unia Europejska zainteresowała się szerzej problemami bezpieczeństwa teleinformatycznego w wyniku poważnych cyberataków na Estonię i Gruzję w latach 2007—2008.

W tym kontekście polityka cyberbezpieczeństwa Unii Europejskiej od początku musiała wziąć pod uwagę szereg poważnych wątpliwości. Przede wszystkim składając się w przeważającej mierze z krajów członkowskich NATO, nie mogła powielić przyjętego przez tę organizację schematu walki z cyberzagrożeniami, powstało więc pytanie, czy istniała jakakolwiek nisza, którą UE mogłaby zagospodarować, nie dublując zarazem kompetencji innych podmiotów międzynarodowych. Z tych dylematów wynikało również pytanie, które instytucje Unii Europejskiej powinny na tego typu wyzwania reagować. Przytoczone wyżej zapisy dawały podstawę zarówno do wykorzystania organów WPZiB, jak i PWBS. Była to kwestia o tyle istotna, iż, jak wiadomo, zagrożenia teleinformatyczne mają zróżnicowany charakter z perspektywy ich politycznych i prawnych konsekwencji. Obawiano się także, że aktywizacja polityki cyberbezpieczeństwa mogłaby w konsekwencji okazać się szkodliwa dla ochrony podstawowych praw człowieka. Jak wspomniała Annegret Bendiek (2012), istniała wątpliwość, czy Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości nie zostałaby zaprzepaszczona przez uznanie za priorytet „właśnie bezpieczeństwa".

W praktyce Unia Europejska zainteresowała się jednak tą sferą stosunkowo późno. Już w latach 90. XX wieku podejmowano inicjatywy zmierzające do rozwoju społeczeństwa informacyjnego oraz przyspieszenia rewolucji informatycznej, o czym świadczyły takie przedsięwzięcia, jak plan działań *Europe's Way to the Information Society. An Action Plan* z 1994 roku czy raport *Living and Working in Information Society. People First* z 1996 roku (szerzej: Siwicki, 2013: 37; Bógdał-Brzezińska, Gawrycki, 2003: 230). Jednak dopiero w 2004 roku, czyli

w dwa lata po NATO, na mocy dyrektywy nr 46/2004[79] podjęto decyzję o utworzeniu pierwszego organu zajmującego się bezpieczeństwem unijnych systemów teleinformatycznych: Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency — ENISA). Stwierdzono w niej, iż

> systemy komunikacji i informacji stały się zasadniczym czynnikiem rozwoju społecznego i gospodarczego. Komputery oraz sieć stają się wszechobecnym dobrem, na takiej samej zasadzie jak elektryczność czy dostęp do wody. Bezpieczeństwo sieci komunikacyjnych i systemów informacyjnych, a w szczególności ich dostępność, jest zatem obiektem rosnącej troski społeczeństwa.

Do głównych zadań Agencji zaliczono:

- wzmocnienie zdolności Wspólnoty, państw członkowskich oraz środowiska biznesowego do zapobiegania i reagowania na problemy bezpieczeństwa informacji i sieci,
- udzielanie pomocy oraz doradztwo Wspólnocie i państwom członkowskim w zakresie bezpieczeństwa informacji i sieci,
- wsparcie narodowych oraz unijnych wysiłków na rzecz osiągnięcia wysokiego poziomu wiedzy w tej dziedzinie,
- stymulowanie kooperacji aktorów sektora publicznego i prywatnego,
- pomoc Komisji Europejskiej w pracach związanych z aktualizacją lub przygotowaniem regulacji prawnych dotyczących bezpieczeństwa informacji i sieci.

W praktyce zadania te ENISA miała realizować m.in. poprzez:

- zbieranie oraz analizę informacji na temat zagrożeń teleinformatycznych,
- udzielanie Komisji Europejskiej, Parlamentowi Europejskiemu oraz innym organom UE doradztwa i wsparcia w wypełnianiu ich funkcji,
- współpracę z różnymi podmiotami w dziedzinie bezpieczeństwa informacji i sieci, w tym np. organizowanie regularnych konsultacji z przedstawicielami przemysłu i środowiska naukowego,
- ułatwianie kontaktów Komisji Europejskiej z krajami członkowskimi poprzez rozwijanie wspólnej metodologii prewencji i zwalczania zagrożeń teleinformatycznych,
- podnoszenie świadomości oraz dostępności informacji na temat wyzwań dla sieci komputerowych i informacji,
- asystowanie KE oraz państwom członkowskim w dialogu z przedstawicielami przemysłu, dotyczącym zarówno bezpieczeństwa sprzętu komputerowego, jak i oprogramowania,

[79] Warto dodać, że już w 2001 roku Komisja Europejska wydała komunikat *Network and Information Security: Proposal for A European Policy Approach*. Mimo wielu ciekawych zapisów i propozycji dokument nie przyniósł jednak żadnych poważnych rezultatów.

- monitorowanie dominujących standardów produktów oraz usług w tej dziedzinie.

Ponadto w artykule 4. dyrektywy zawarto podstawowe definicje będące fundamentem dalszych działań UE na tym polu. Scharakteryzowano tu m.in. takie terminy, jak *sieć*, *system informacyjny*, *bezpieczeństwo informacji i sieci*, *integralność danych* czy *zarządzanie ryzykiem*. W kolejnych punktach określono także dokładną strukturę ENISA, która miała się składać z Zarządu (Management Board), Dyrektora Wykonawczego (Executive Director) oraz Stałej Grupy Interesariuszy (Permanent Stakeholders' Group) (*Regulation (EC) No 460/2004*).

W tym kontekście należy podkreślić, iż chociaż już wcześniej dyrektywy UE poruszały w mniejszym lub większym stopniu problematykę cyberbezpieczeństwa, dopiero ta z 2004 roku otworzyła nowy rozdział tych prac, ponieważ dokument powołujący ENISA był dobrze przemyślany i bogaty w treść. Był on zarazem pierwszym sygnałem, że Unia Europejska będzie dążyła jedynie do uzupełnienia i wsparcia aktywności innych podmiotów na arenie międzynarodowej.

Pomimo tych zapisów Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji przez kolejne kilka lat wykazywała jednak niewielką aktywność. Wynikało to prawdopodobnie z trzech powodów. Po pierwsze cyberbezpieczeństwo było nadal traktowane w Unii Europejskiej jako sprawa drugorzędnej wagi, podobnie zresztą jak w innych organizacjach międzynarodowych. Po drugie trwały wówczas prace nad reformą instytucjonalną UE, tak specjalistyczne zagadnienia musiały zatem zejść na dalszy plan. Po trzecie same zapisy dyrektywy nr 46/2004 świadczyły o tym, iż to państwa członkowskie miały być głównymi podmiotami odpowiedzialnymi za zwalczanie zagrożeń teleinformatycznych. W tej sytuacji kolejna ważniejsza inicjatywa Unii miała miejsce dopiero w 2006 roku. W maju Komisja Europejska wydała komunikat pt. *A Strategy for a Secure Information Society — „Dialogue, partnership and empowerment"* (2006). Myślą przewodnią tego dokumentu, choć nie wyrażono tego w sposób bezpośredni, było skonkretyzowanie kompetencji Unii Europejskiej. Była to zarazem próba rewitalizacji europejskiej polityki cyberbezpieczeństwa. We wstępie stwierdzono, iż celem tego dokumentu jest „rozwój dynamicznej, globalnej strategii dla Europy, bazującej na kulturze bezpieczeństwa oraz ufundowanej na dialogu, partnerstwie i upodmiotowieniu". W rozdziale drugim wskazano kluczowe wyzwania, przed którymi stała wówczas UE. Zwrócono tu m.in. uwagę na fakt, że cyberataki coraz częściej motywowane są chęcią zysku. W tym kontekście stwierdzono, iż polityka cyberbezpieczeństwa powinna być oparta na takich wartościach, jak otwartość, różnorodność oraz interoperacyjność. Podkreślono ponadto zasadnicze znaczenie technologii oraz sektora ICT dla gospodarki europejskiej. Jako dowód przytoczono informacje, według których w 2004 roku aż 89% przedsiębiorstw unijnych korzystało aktywnie z Internetu. W związku z tym w rozdziale trzecim Komisja Europejska zaproponowała „dynamiczną i zintegrowaną" poli-

tykę bezpieczeństwa teleinformatycznego, ufundowaną m.in. na dialogu z interesariuszami. Wśród składających się nań inicjatyw wymieniono zwalczanie spamu oraz złośliwych programów komputerowych (*spyware*), a także podnoszenie poziomu kooperacji pomiędzy organami ścigania. Zaproponowano także stworzenie, przy wykorzystaniu ENISA, europejskiego wielojęzykowego systemu alarmowego oraz wymiany informacji, który zostałby oparty na istniejących już strukturach i rozwiązaniach z sektora publicznego i prywatnego. Wskazano ponadto na potrzebę pogłębiania globalnej współpracy na tym polu, realizując ustalenia Światowego Szczytu Społeczeństwa Informacyjnego (WSIS). Podkreślono też znaczenie prac badawczo-rozwojowych, które powinny być prowadzone na poziomie europejskim. Powyższy dokument KE z pewnością prawidłowo, choć bardzo ogólnie identyfikował wyzwania dla bezpieczeństwa teleinformatycznego Starego Kontynentu, co ważne: jeszcze przed wydarzeniami w Estonii i Gruzji. Sygnalizował on zarazem, w jakim kierunku będzie ewoluować unijna polityka w tym zakresie. Komunikat pominął w zasadzie w całości cyberzagrożenia, które wiązałyby się z jakimikolwiek konsekwencjami politycznymi lub wojskowymi, skupił się natomiast wyłącznie na cyberprzestępczości, co dowodziło chęci uniknięcia dublowania struktur i kompetencji Sojuszu Północnoatlantyckiego.

Powyższa strategia, podobnie jak wcześniejsze tego typu dokumenty i deklaracje, nie doprowadziła jednak do znaczącego zintensyfikowania prac Unii Europejskiej w tej dziedzinie. Co prawda podejmowano tutaj pewne inicjatywy, lecz miały one bardzo ograniczony charakter (*Commission decision*, 2006). Do znaczącej zmiany doszło dopiero po omówionych już incydentach teleinformatycznych w Estonii. Już w maju 2007 roku Komisja Europejska wydała komunikat, w którym zwrócono się do innych organów UE o opracowanie strategii zwalczania cyberprzestępczości. W komunikacie zdefiniowano przede wszystkim, czym jest przestępczość komputerowa, wyróżniając jej trzy rodzaje: zamieszczanie online nielegalnych materiałów, konwencjonalne przestępstwa przy wykorzystaniu środków elektronicznych oraz takie akty, które są unikalne tylko dla środowiska teleinformatycznego (cyberataki). Zauważono ponadto nie tylko rosnącą liczbę oraz poziom zaawansowania incydentów teleinformatycznych o podłożu kryminalnym, ale również coraz większe zainteresowanie zorganizowanych grup przestępczych cyberprzestrzenią. W związku z tym stwierdzono, iż „w świetle tego zmieniającego się środowiska pojawiła się paląca potrzeba podjęcia działań — zarówno na narodowym, jak i europejskim poziomie — przeciwko wszelkim formom cyberprzestępczości, które stanowią coraz poważniejsze zagrożenie dla infrastruktury krytycznej, społeczności, biznesu oraz obywateli". Celem dokumentu było więc:

- ułatwienie i usprawnienie kooperacji i koordynacji między organami zwalczającymi cyberprzestępczość w państwach członkowskich, jak również między innymi strukturami i ośrodkami eksperckimi w Unii Europejskiej,

- opracowanie wraz z państwami członkowskimi, a także odpowiednimi organami międzynarodowymi i unijnymi ram skutecznej polityki zwalczania przestępczości komputerowej,
- podniesienie świadomości na temat zagrożeń wynikających z tego zjawiska.

W związku z tym Komisja Europejska zaproponowała szereg przedsięwzięć, które miały przyczynić się do realizacji powyższych priorytetów. Przede wszystkim zasugerowano zintensyfikowanie współpracy państw UE w zakresie zwalczania cyberprzestępczości przy użyciu takich struktur, jak EUROPOL czy EUROJUST. Po drugie wskazano na potrzebę zainicjowania programów szkoleniowych w tej dziedzinie, wykorzystując tu np. Europejską Sądową Sieć Szkoleniową (European Judicial Training Network — EJTN). Po trzecie zadeklarowano, iż KE zorganizuje spotkanie ekspertów z państw członkowskich oraz organów unijnych, którego celem miało być pogłębienie strategicznych kontaktów w tej dziedzinie. Po czwarte podkreślono znaczenie prowadzenia pogłębionego dialogu między sektorem publicznym i prywatnym, m.in. w formie spotkań przedstawicieli organów ścigania z takimi podmiotami, jak dostawcy usług internetowych. Po piąte wspomniano również o potrzebie ograniczonej współpracy prawnej, jeśli chodzi o kradzież tożsamości. Po szóste zaakcentowano wagę zbierania danych statystycznych na ten temat. Zauważając, iż inicjatywy Komisji Europejskiej mogą jedynie uzupełniać politykę państw członkowskich, wyróżniono szereg zadań na przyszłość, takich jak wspieranie badań naukowych nad cyberprzestępczością, promowanie globalnej współpracy czy wspieranie ratyfikacji *Konwencji Rady Europy o cyberprzestępczości* (*Towards a general policy*, 2007). Dokument ten miał więc kilka interesujących cech i był stosunkowo szybką reakcją na kryzys w Estonii. Potwierdził ponadto, iż Unia Europejska zamierza jedynie wspierać i uzupełniać działania na szczeblu narodowym. Udowodnił także, iż Komisja była zainteresowania zwalczaniem przestępczości komputerowej, pomijając inne rodzaje zagrożeń.

Choć sam komunikat KE zawierał szereg ważnych spostrzeżeń, to ponownie nie przełożył się na praktyczną współpracę. Dopiero w czerwcu 2008 roku rozpoczęto interesujący program *Safer Internet Plus*[80], który przewidywał m.in. walkę z nielegalną zawartością Internetu, walkę ze spamem czy podnoszenie świadomości internautów na temat wyzwań pojawiających się online[81]. Niedługo później, w listopadzie, Komisja Europejska rozpoczęła publiczne konsultacje na temat priorytetów polityki bezpieczeństwa informacji i sieci. Komisarz Viviane Reding wezwała wówczas Parlament Europejski oraz Radę do rozpoczęcia od 2009 roku intensywnej debaty na temat tego, w jaki sposób UE może reagować

[80] Przy czym warto pamiętać, iż już od 1999 roku działał program Komisji Europejskiej *Safe Internet*. Zob. *Safe Internet*: www.saferinternet.pl/pl; dostęp: 17.03.2014.

[81] *Making the Internet a safer place*. European Commission. Information Society and Media, June 2008: http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus-en.pdf; dostęp: 17.03.2014.

na cyberataki, uwzględniając przy tym ENISA[82]. Rzeczywiście, już w marcu tego roku podjęto kolejną inicjatywę w tej dziedzinie: Komisja Europejska wydała wówczas komunikat, który został poświęcony w całości ochronie infrastruktury krytycznej przed włamaniami komputerowymi na dużą skalę (*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, 2009). We wstępie do niego zauważono rosnące uzależnienie państw i społeczeństw od prawidłowego działania technologii informacyjnych i komunikacyjnych. Podkreślono również doniosłe konsekwencje ewentualnego zakłócenia funkcjonowania infrastruktury krytycznej państw dla gospodarki światowej. Dalej stwierdzono, iż wszelkie pomysły zawarte w tym dokumencie będą realizowane w ramach europejskiego programu ochrony infrastruktury krytycznej (*European Programme For Critical Infrastructure Protection*). Przypomniano zarazem, iż KE w pracach nad dokumentem wzięła pod uwagę politykę cyberbezpieczeństwa NATO oraz rezolucję Zgromadzenia Ogólnego ONZ nr 58/199 poświęconą globalnej kulturze cyberbezpieczeństwa. W punkcie 3. komunikatu autorzy omówili znaczenie funkcjonalności infrastruktury krytycznej dla bezpieczeństwa Unii Europejskiej, przywołując m.in. przykłady Estonii, Litwy oraz Gruzji. W tym kontekście oprócz samych cyberataków do głównych wyzwań dla Europy zaliczono m.in. brak koordynacji między poszczególnymi państwami członkowskimi, brak zarządzania (*governance*) ochroną infrastruktury informacyjnej na poziomie europejskim i ograniczone zdolności wczesnego ostrzegania o incydentach. W związku z tym główną myślą przewodnią dokumentu było pogłębienie współpracy w Unii w oparciu o pięć „filarów" zakładających:

- zdefiniowanie podstawowych standardów, zdolności i usług dla paneuropejskiej kooperacji, głównie między narodowymi zespołami CERT,
- opracowanie Europejskiego Systemu Alarmowego i Wymiany Informacji (European Information Sharing and Alert System — EISAS),
- przygotowanie narodowych planów awaryjnych, organizację regularnych ćwiczeń z udziałem zespołów CERT i ENISA, a także pogłębianie kontaktów między samymi zespołami CERT,
- promowanie ogólnoeuropejskiej debaty na ten temat (z uwzględnieniem sektora prywatnego) i zdefiniowanie podstawowych zasad stabilności i odporności Internetu,
- określenie podstawowych kryteriów identyfikacji europejskiej infrastruktury krytycznej w sektorze ICT.

W podsumowaniu stwierdzono, iż ochrona krytycznej infrastruktury informacyjnej jest niezbędna, aby czerpać pełne korzyści z funkcjonowania społe-

[82] *Commission launches public consultation on network and information society*. Europe's Information Society, 07.11.2008: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464; dostęp: 17.03.2014.

czeństwa informacyjnego. Warto dodać, iż reagując na ten ważny dokument w grudniu 2009 roku, ENISA określiła po raz pierwszy w historii podstawowy zestaw rekomendacji i sugestii dla narodowych zespołów reagowania na incydenty komputerowe (CERT) (zob. *Baseline capabilities*, 2009).

Kolejny krok wskazujący na rosnące znaczenie tematyki cyberbezpieczeństwa dla UE został poczyniony w maju 2010 roku, kiedy przyjęto *Digital Agenda for Europe*. We wprowadzeniu do niej stwierdzono wyraźnie, iż jej celem jest „wytyczenie drogi pozwalającej na maksymalne wykorzystanie ekonomicznego i społecznego potencjału TIK [technologii informacyjno-komunikacyjnych — M.L.], w szczególności internetu, który stanowi ważny środek działalności gospodarczej i społecznej". W dalszej części dodano:

> Europejczycy nie będą chcieli angażować się w coraz bardziej złożoną działalność internetową, o ile nie będą mieć pewności, że oni sami lub ich dzieci mogą w pełni polegać na sieci. Dlatego Europa musi zająć się nową formą przestępczości — „cyberprzestępczością" — obejmującą między innymi wykorzystywanie dzieci, kradzież tożsamości i ataki cybernetyczne — oraz musi opracować odpowiednie mechanizmy reakcji.

W związku z tym w punkcie 2.3 agendy wymieniono szereg działań, które powinny zapewnić bezpieczeństwo europejskich sieci komputerowych oraz ich użytkowników:

- prowadzenie udoskonalonej polityki w zakresie bezpieczeństwa informacji i sieci, co miało się przejawiać np. unowocześnieniem Agencji ds. Bezpieczeństwa Sieci i Informacji,
- użycie środków, w tym inicjatyw ustawodawczych, ukierunkowanych na zwalczanie cyberataków na szczeblu europejskim i międzynarodowym,
- ustanowienie do 2012 roku europejskiej platformy walki z cyberprzestępczością,
- przeprowadzenie analizy możliwości ustanowienia europejskiego centrum ds. walki z cyberprzestepczością do 2011 roku,
- pogłębianie współpracy międzynarodowej,
- aktualizacja unijnych ram prawnych.

Ponadto zobowiązano państwa członkowskie do ustanowienia dobrze działającej sieci narodowych zespołów CERT, przeprowadzenia przy współpracy z KE symulacji cyberataku na dużą skalę oraz wdrożenia specjalnych numerów telefonów do powiadamiania o szkodliwych treściach online (*Europejska Agenda Cyfrowa*, 2010).

Potwierdzeniem wyznaczonych w DAE priorytetów były działania, które Komisja Europejska podjęła na początku 2011 roku. W marcu przyjęto następny komunikat na temat dotychczasowych osiągnięć oraz kolejnych kroków w kierunku „globalnego cyberbezpieczeństwa" (*Achievements and next steps: towards*

global cyber-security, 2011). Dokument ten nawiązał do zainicjowanych już działań związanych z ochroną infrastruktury krytycznej, a także zapisów agendy cyfrowej. Znalazło się w nim odniesienie do innych niż zwykle typów zagrożeń teleinformatycznych: cyberterroryzmu oraz cyberwojny, choć kwestie te omówiono bardzo ogólnikowo. W punkcie 4. wymieniono najważniejsze dotychczasowe przedsięwzięcia UE z zakresu ochrony infrastruktury krytycznej: aktywność Europejskiego Forum Państw Członkowskich (European Forum of Member States), powołanie europejskiego partnerstwa publiczno-prywatnego (European Public-Private Partnership for Resilience), opracowanie przez ENISA mapy drogowej rozwoju Europejskiego Systemu Alarmowego i Wymiany Informacji czy przeprowadzenie pierwszego paneuropejskiego ćwiczenia z zakresu cyberbezpieczeństwa 4 listopada 2010 roku (*Cyber Europe 2010*). Uczestniczyły w nich wszystkie państwa członkowskie (z czego 19 aktywnie), jak również Szwajcaria, Norwegia i Islandia. W punkcie 5. wskazano na najważniejsze inicjatywy, które Komisja Europejska miała podjąć w przyszłości. Przede wszystkim zamierzała ona nadal promować podstawowe zasady „stabilności i elastyczności" Internetu w środowisku międzynarodowym. Po drugie jej celem była budowa sieci „strategicznych partnerstw" w takich obszarach, jak zarządzanie incydentami komputerowymi czy współpraca zespołów CERT. Uznano przy tym, iż istotnym krokiem w celu urzeczywistnienia tego planu było stworzenie w listopadzie 2010 roku wspólnej amerykańsko-europejskiej grupy roboczej ds. cyberbezpieczeństwa i cyberprzestępczości (EU-US Working Group on Cyber-security and Cyber--crime). Po trzecie wspomniano o intensyfikacji debaty na temat najnowszych technologii teleinformatycznych, w tym np. *cloud computingu*. W tym kontekście wyznaczono także trzy zadania do realizacji dla krajów członkowskich: utworzenie sieci skutecznie działających krajowych zespołów CERT do 2012 roku, opracowanie wraz z ENISA europejskiego planu awaryjnego na wypadek incydentów teleinformatycznych oraz skoordynowanie aktywności na forum międzynarodowym. Co jednak najważniejsze, stwierdzono, iż istniała potrzeba zrównoważenia dotychczasowej debaty na ten temat, która nadmiernie skoncentrowała się na problematyce bezpieczeństwa narodowego oraz kwestiach wojskowych. Świadczyło to więc wyraźnie o odmiennej specyfice polityki cyberbezpieczeństwa Unii Europejskiej, która w zdecydowanie większym stopniu skupiała się na takich kwestiach, jak zwalczanie cyberprzestępczości, walka z kradzieżą tożsamości i nielegalnymi materiałami online czy ochrona praw człowieka w sieci.

Do dalszej intensyfikacji prac Unii Europejskiej doszło w 2012 roku. Przejawiało się to na kilka sposobów. W marcu Komisja Europejska wydała komunikat poświęcony powołaniu w ramach EUROPOL-u Europejskiego Centrum Cyberprzestępczości (European Cybercrime Center). Zaczęło ono oficjalnie funkcjonować 1 stycznia 2013 roku. Zauważając rosnącą skalę zagrożeń teleinformatycznych, w komunikacie zaproponowano stworzenie EC3, które respektując zasadę subsydiarności, miało zajmować się przestępstwami komputero-

wymi popełnionymi przez zorganizowane grupy przestępcze czerpiące z tego procederu duże zyski (np. oszustwa online), cyberprzestępstwami, które mogą wyrządzić poważne szkody potencjalnym ofiarom (np. wykorzystanie dzieci), aktami wpływającymi na funkcjonowanie infrastruktury krytycznej oraz systemów informacyjnych UE (cyberataki).

W związku z tym przed EC3 wyznaczono cztery główne funkcje. Po pierwsze miało służyć jako punkt wymiany informacji na temat przestępczości komputerowej, zbierając dane ze źródeł publicznych, prywatnych oraz ogólnodostępnych. W założeniu powinno to prowadzić do podnoszenia zdolności do zwalczania lub prewencji cyberzagrożeń. Po drugie EC3 miało wspierać kraje członkowskie w prowadzeniu analiz, ćwiczeń i szkoleń z zakresu przeciwdziałania cyberprzestępczości. Po trzecie powinno wspomagać je w dochodzeniach związanych z tego typu aktami. Po czwarte do zadań centrum zaliczono reprezentowanie europejskiego punktu widzenia w debatach na arenie międzynarodowej. W praktyce EC3 nawiązało współpracę nie tylko z państwami członkowskimi, ale także wybranymi organizacjami, środowiskiem naukowym oraz rozmaitymi podmiotami pozapaństwowymi. Wśród jego najciekawszych projektów należy wymienić m.in. Bezpieczny Dzień w Internecie (*Safe Internet Day*), prowadzenie szkoleń, udostępnianie specjalistycznej infrastruktury teleinformatycznej czy organizację Centrum Fuzji Danych (Data Fusion Center), odpowiedzialnego za zbieranie informacji na temat cyberprzestępczości[83].

Wyrazem większego zainteresowania UE zagrożeniami teleinformatycznymi były również operacje przeprowadzone przez EUROPOL. W 2011 roku zakończyła się np. trzyletnia kampania *Rescue*, w której wyniku zatrzymano 184 osoby należące do globalnej siatki pedofilów[84]. W 2012 roku przeprowadzono natomiast operację *Atlantic*, w której wyniku zidentyfikowano kolejnych 37 pedofilów[85]. Ponadto w 2012 roku większą niż dotychczas aktywność zaczęła wykazywać Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji. Wyrazem tego było ogłoszenie w październiku europejskiego miesiąca cyberbezpieczeństwa. Głównym założeniem tej inicjatywy było podnoszenie świadomości opinii publicznej na temat wyzwań dla infrastruktury teleinformatycznej. Europejski miesiąc cyberbezpieczeństwa został powtórzony w roku 2013[86]. W tym samym cza-

[83] *Tackling Crime*, 2012; *European Cybercrime Center*. EUROPOL: www.europol.europa.eu/ec3/services; dostęp: 19.03.2014.

[84] K. McVeigh: *Police shut down global paedophile network in Operation Rescue*. „The Guardian" 16.03.2011: www.theguardian.com/society/2011/mar/16/global-paedophile-ring-smashed; dostęp: 19.03.2014.

[85] *European police and FBI dismantle network of child sex offenders*. EUROPOL, 29.02.2012: www.europol.europa.eu/content/press/european-police-and-fbi-dismantle-network-child-sex-offenders-1361; dostęp: 19.03.2014.

[86] *European Cyber Security Month*. ENISA: http://cybersecuritymonth.eu; dostęp: 19.03.2014.

sie wsparto prace naukowo-badawcze w tej dziedzinie, w listopadzie 2012 roku Komisja Europejska zadeklarowała bowiem podniesienie wydatków na ten cel z 350 mln euro w latach 2007—2013 do 400 mln euro w latach 2014—2020. Do tego należy dodać ok. 450 mln euro w ramach programu *Secure Societies*, co oznaczało wzrost nakładów na badania o ok. 14%. Wśród najważniejszych finansowanych w ten sposób programów należy wymienić m.in.: *Syssec*, *Nessos*, *SecureChange*, a także *Tclouds*[87]. W 2012 roku problemami cyberbezpieczeństwa szerzej zainteresowały się inne niż dotychczas organy Unii Europejskiej. Świadczyło o tym wystąpienie Catherine Ashton, wysokiej przedstawiciel Unii ds. zagranicznych i polityki bezpieczeństwa, na konferencji w Budapeszcie 4 października 2012 roku. Zauważyła ona wówczas, iż bezpieczeństwo cyberprzestrzeni ma znaczenie nie tylko w wymiarze ekonomicznym, lecz również społecznym i politycznym, czego dowodem była arabska wiosna. Zaakcentowała ponadto, iż rosnące uzależnienie społeczeństw od ICT jest czynnikiem, który sprzyja większemu zainteresowaniu cyberprzestrzenią przez „niszczycielskie siły". Aby to zobrazować, przywołała badania, według których aż 29% Europejczyków nie czuło się bezpiecznie w sieci. W związku z tym padło kilka ważnych deklaracji. Catherine Ashton wskazała na palącą potrzebę ustalenia norm zachowania państw w sieci oraz zadeklarowała, iż Unia Europejska jest zdeterminowana, aby bronić i promować reprezentowane przez siebie wartości w wymiarze online. Chodziło tu przede wszystkim o kwestię ochrony praw człowieka (Ashton, 2012).

Potwierdzeniem tych tendencji była aktywizacja Parlamentu Europejskiego. W listopadzie 2012 roku opublikowano raport przygotowany przez eurodeputowanego Tunnego Kelama, który ostro skrytykował dotychczasowe zaniedbania w polityce europejskiej na tym obszarze. Zauważył w nim, iż Unia Europejska nie miała w zasadzie pełnego, wyczerpującego oglądu całej gamy zagrożeń teleinformatycznych. Brakowało nie tylko lepszej koordynacji i współpracy w tej dziedzinie, ale również kwestii fundamentalnych, takich jak wspólne definicje oraz standardy zwalczania cyberataków. W raporcie zwrócono większą niż dotychczas uwagę na znaczenie motywowanych politycznie incydentów komputerowych. W związku z tym zaproponowano szereg działań naprawczych, do których zaliczono budowę zaufania między państwami członkowskimi a sektorem prywatnym, szybkie zakończenie prac nad narodowymi strategiami cyberbezpieczeństwa, poszerzenie kompetencji ENISA oraz zajęcie się tą problematyką przez europejską dyplomację, głównie w stosunkach transatlantyckich[88]. Ponadto w listopadzie 2012 roku również inni eurodeputowani zainteresowali się tematyką cyberbezpieczeństwa. W przyjętej wówczas rezolucji wskazano, że Unia Europejska powinna dostosować się do nowych, globalnych zagrożeń dla

[87] J. Baker: *EU's cybersecurity budget up 14%*. „Computer World" 26.11.2012: www.computerworld.com.au/article/442917/eu_cybersecurity_budget_up_14_; dostęp: 19.03.2014.

[88] *EU Cyber Security and Defence: time to act now!* EPP Group, 22.11.2012: www.eppgroup.eu/press-release/EU-Cyber-Security-and-Defence%3A-time-to-act-now!-; dostęp: 19.03.2014.

jej bezpieczeństwa. W związku z tym zasugerowano wykorzystanie instrumentów Wspólnej Polityki Bezpieczeństwa i Obrony do rozwinięcia swojego potencjału obronnego w cyberprzestrzeni[89].

Na tym tle najistotniejszym wydarzeniem w 2012 roku było z pewnością powołanie 1 września Zespołu Reagowania na Incydenty Komputerowe Unii Europejskiej (Computer Emergency Response Team — CERT-UE). Głównym zadaniem tej nowej struktury stało się „wspieranie europejskich instytucji w ich ochronie przeciwko intencjonalnym i złośliwym atakom, które zakłóciłyby integralność ich zasobów teleinformatycznych oraz zaszkodziły interesom Unii Europejskiej". CERT-UE miał zatem działać w czterech sferach (prewencji, wykrywania, odpowiedzi i odzyskiwania) w oparciu o szereg zasad: najwyższych standardów „etycznej integralności", wysokiego poziomu gotowości operacyjnej, skutecznej odpowiedzi w wypadku incydentów, ułatwiania wymiany dobrych praktyk oraz wzmacniania „kultury otwartości". W praktyce oznaczało to m.in. publikowanie ogłoszeń i ostrzeżeń o pojawiających się w sieci zagrożeniach oraz koordynację odpowiedzi na cyberataki w ramach instytucji europejskich. Warto dodać, iż CERT-UE składał się z ekspertów ds. zabezpieczeń komputerowych pochodzących ze wszystkich głównych organów UE: Komisji, Sekretariatu Generalnego Rady, Parlamentu Europejskiego czy Komitetu Regionów[90]. Decyzję tę można było postrzegać jako realizację wielu postulatów, które pojawiły się m.in. w agendzie cyfrowej, dziwi jednak fakt, iż instytucję o tak fundamentalnym znaczeniu dla bezpieczeństwa teleinformatycznego Unii Europejskiej powołano tak późno.

Bez względu na te wątpliwości przełom, który wówczas nastąpił, został potwierdzony w roku następnym. 7 lutego 2013 roku przyjęto *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Jak zauważyła Catherine Ashton, dokument ten stał się wyrazem determinacji Europy, aby zapewnić ochronę podstawowych praw człowieka w przestrzeni teleinformatycznej (*Remarks by EU*, 2013). We wstępie, odwołując się m.in. do przykładu arabskiej wiosny, podkreślono zasadniczy wpływ funkcjonowania Internetu na różne dziedziny życia człowieka. Wskazano, że uniwersalne wartości, takie jak demokracja, wolność słowa czy rządy prawa muszą być przestrzegane również w cyberprzestrzeni, powinna ona być zatem chroniona przed wszelkimi szkodliwymi aktami. Zauważono przy tym, że cyberzagrożenia mają charakter wielowymiarowy i rozciągają się od przestępczości komputerowej, przez akty cyberterroryzmu, aż po działalność sponsorowaną przez poszczególne państwa. W związku z tym powstała paląca potrzeba uregulowania stosunku Unii Europejskiej do tych zagadnień. W punkcie 1.2 wyznaczono podstawowe wartości,

[89] T. Smith: *EU must bolster its cyber security say MEPs*. CBR, 23.11.2012: www.cbronline.com/news/eu-must-bolster-its-cyber-security-say-meps-231112; dostęp: 19.03.2014.

[90] *RFC 2350*, 2012; *About us*, CERT-EU: http://cert.europa.eu/cert/plainedition/en/cert_about.html; dostęp: 19.03.2014.

którymi powinna się kierować UE. Wymieniono tu ochronę podstawowych praw człowieka, w tym swobody wypowiedzi i prawa do prywatności, zapewnienie dostępu do Internetu dla wszystkich obywateli, demokratyczne i uwzględniające sektor prywatny zarządzanie siecią oraz wspólną odpowiedzialność za bezpieczeństwo cyberprzestrzeni.

Do głównych priorytetów strategii zaliczono:

- osiągnięcie „cyberodporności" m.in. poprzez:
  - — opracowanie wspólnych minimalnych wymogów w zakresie cyberbezpieczeństwa,
  - — ustanowienie mechanizmów prewencji, wykrywania oraz zwalczania zagrożeń komputerowych,
  - — podnoszenie poziomu zaangażowania oraz przygotowania sektora prywatnego (np. poprzez European Public-Private Partnership for Resilience),
  - — rozpoczęcie programu zwalczania sieci *botnet* oraz złośliwego oprogramowania od 2013 roku,
  - — prowadzenie regularnych, paneuropejskich ćwiczeń w sieci,
  - — przyjęcie dyrektywy poświęconej europejskiej współpracy w tym zakresie,
  - — dalszą organizację „miesiąca cyberbezpieczeństwa" przez ENISA,
  - — promocję działań podnoszących świadomość skali cyberzagrożeń;
- drastyczne zredukowanie cyberprzestępczości poprzez:
  - — promocję ratyfikacji *Konwencji Rady Europy o cyberprzestępczości*,
  - — ustalenie wraz z państwami członkowskimi systemu dobrych praktyk,
  - — przydzielenie państwom członkowskim dodatkowych funduszy na przeciwdziałanie wyzwaniom teleinformatycznym,
  - — wsparcie dla Europejskiego Centrum Cyberprzestępczości,
  - — lepszą koordynację polityki cyberbezpieczeństwa na poziomie unijnym,
  - — uczestniczenie w Global Alliance against Child Sexual Abuse Online;
- rozwój polityki cyberobronnej w ramach Wspólnej Polityki Bezpieczeństwa i Obrony za pomocą następujących działań:
  - — opracowania doktryny i ram organizacyjnych, a także stworzenia odpowiedniej infrastruktury, technologii oraz zatrudnienia personelu,
  - — ochrony sieci wykorzystywanych w operacjach WPBiO,
  - — dialogu i kooperacji między podmiotami wojskowymi i cywilnymi,
  - — dialogu z partnerami międzynarodowymi, w tym przede wszystkim Sojuszem Północnoatlantyckim, co pozwoliłoby m.in. na uniknięcie dublowania kompetencji;
- rozwój przemysłowych i technologicznych zasobów poprzez:
  - — promocję wysokich standardów bezpieczeństwa teleinformatycznego w procesach produkcji przemysłowej i technologicznej,
  - — analizę, w jaki sposób producenci sprzętu komputerowego oraz oprogramowania mogliby współpracować z rządami co do wykrywania i informowania o lukach w zabezpieczeniach swoich produktów,

  - — stworzenie przy pomocy ENISA zestawu standardów, rekomendacji i wskazówek dla producentów sektora ICT,
  - — intensyfikację programów badawczo-rozwojowych w tej dziedzinie;
- ustanowienie spójnej polityki cyberbezpieczeństwa UE na arenie międzynarodowej, która promowałaby jej najważniejsze wartości; wśród głównych inicjatyw wymieniono:
  - — uwzględnienie tych zagadnień w działaniach Europejskiej Służby Działań Zewnętrznych oraz Wspólnej Polityce Zagranicznej i Bezpieczeństwa,
  - — wspieranie prac nad określeniem podstawowych norm zachowania w cyberprzestrzeni,
  - — ochronę praw człowieka w środowisku teleinformatycznym,
  - — podnoszenie stopnia koordynacji oraz wymiany informacji między sieciami ochrony infrastruktury krytycznej (CIIP),
  - — wspieranie dostępu do informacji oraz Internetu.

W tym kontekście wyznaczono trzy grupy instytucji odpowiedzialnych za realizację tych zadań. Pierwszą były te, które posiadały kompetencje związane z bezpieczeństwem sieci i informacji. Wymieniono tu Komisję Europejską, ENISA, a także CERT-EU. Do drugiej, odpowiedzialnej za walkę z przestępczością komputerową, zaliczono EUROPOL/EC3, CEPOL oraz EUROJUST. Wśród instytucji trzeciej grupy pełniącej funkcje związane z cyberobroną wymieniono EEAS oraz Europejską Agencję Obrony. Wszystkie te organy zgodnie z zapisami strategii powinny współpracować ze swoimi odpowiednikami na poziomie narodowym. Najważniejsze i konstytutywne dla tego dokumentu zapisy zawarto jednak w punkcie 3.2, dotyczącym reakcji Unii Europejskiej na poważny incydent lub atak teleinformatyczny na któreś z państw członkowskich. Przewidziano tam możliwość nie tylko wymiany informacji między właściwymi instytucjami, ale także praktycznego wsparcia, np. likwidacji skutków włamania. Ponadto jeśli cyberatak miałby charakter przestępczy, wówczas kraj członkowski powinien poinformować o tym EUROPOL, który mógłby włączyć się w dochodzenie, w tym zbieranie dowodów czy identyfikację sprawców. Jeśli cyberatak miałby charakter szpiegowski, byłby przeprowadzony przez obce państwo lub wiązałby się z poważnymi konsekwencjami dla bezpieczeństwa narodowego, wówczas UE przewidziała możliwość zastosowania europejskiej klauzuli solidarności, uregulowanej przez artykuł 222. traktatu o funkcjonowaniu Unii Europejskiej (*Cybersecurity Strategy EU*, 2013). Zgodnie z jego zapisami

> Unia i jej Państwa Członkowskie działają wspólnie w duchu solidarności, jeżeli jakiekolwiek Państwo Członkowskie stanie się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej lub katastrofy spowodowanej przez człowieka. Unia mobilizuje wszystkie będące w jej dyspozycji instrumenty,

> w tym środki wojskowe udostępnione jej przez Państwa Członkowskie, w celu […] zapobiegania zagrożeniu terrorystycznemu na terytorium Państw Członkowskich, […] udzielenia pomocy Państwu Członkowskiemu na jego terytorium, na wniosek jego władz politycznych, w przypadku klęski żywiołowej lub katastrofy spowodowanej przez człowieka.

Należy stwierdzić, iż opisana wyżej strategia stała się solidnym fundamentem dojrzałej europejskiej polityki bezpieczeństwa teleinformatycznego, w sposób przemyślany regulując najbardziej palące kwestie. Na szczególną uwagę zasługuje tu kilka spraw. Przede wszystkim warto zwrócić uwagę na fakt, iż cyberbezpieczeństwo uwzględniono jako jeden z priorytetów działań zewnętrznych Unii. Tym samym UE miała stać się jednym z aktywniejszych podmiotów wspierających prace nad podstawowymi regulacjami w tej dziedzinie w oparciu o takie rozwiązania, jak *Konwencja Rady Europy o cyberprzestępczości*. Po drugie zasadniczą nowością w stosunku do wcześniejszych dokumentów był zapis o rozwijaniu zdolności cyberobronnych UE. Mogło to świadczyć o chęci poszerzenia zakresu Wspólnej Polityki Bezpieczeństwa i Obrony, wyraźnie jednak stwierdzono, iż UE nie chce duplikować kompetencji NATO, tym bardziej, iż zakres inicjatyw w tej dziedzinie okazał się stosunkowo wąski. Za najważniejszy element strategii należy uznać punkt 3.2, w którym sprecyzowano sposób reakcji UE na cyberataki. Zapisy o wsparciu w przypadku wystąpienia aktów cyberprzestępczości były ważne, lecz dość standardowe. Zasadniczym *novum* okazała się natomiast decyzja o możliwości uruchomienia klauzuli solidarności w wypadku cyberataków zorganizowanych przez obce państwo. Ten mechanizm należy uznać za przełomowy z dwóch powodów. Przede wszystkim udowodnił on, iż Unia Europejska po wielu latach zaczęła w końcu zwracać większą uwagę na inny typy wyzwań pojawiających się w cyberprzestrzeni: cyberwojnę, cyberterroryzm oraz cyberszpiegostwo, sugerowało to ponadto, iż UE nie będzie chciała dopuścić do powtórki sytuacji z Estonii z 2007 roku.

Nie był to jednak dokument pozbawiony błędów. Jak pisał Piotr Rutkowski (2014: 57), pominięto w nim wiele istotnych zagadnień:

> Proponowana obecnie Strategia nie pasuje do charakteru i zakresu zagrożeń związanych z powszechną dostępnością technologii informacyjnych. Nie odpowiada na bieżące problemy, związane z ryzykiem wykorzystania w sposób nieczysty rynkowej przewagi, nie uwzględnia zagrożeń związanych z naturalnym ryzykiem wtórnych skutków awarii i katastrof w systemach, które zależą od wykorzystania technologii informacyjnych. To podejście zupełnie inne niż np. obecne planowanie w Stanach Zjednoczonych.

Bez względu na te zarzuty można jednak zaryzykować stwierdzenie, iż przynajmniej w wymiarze deklaratywnym Unia Europejska w 2013 roku znalazła

się, obok NATO, w czołówce organizacji regionalnych zajmujących się problematyką cyberbezpieczeństwa. Warto również zauważyć, iż na kanwie tego dokumentu w latach 2013/2014 zaczęto realizować szereg interesujących przedsięwzięć. Należy tu wymienić m.in.:

- rozpoczęcie projektu *Tabula Rasa*, dotyczącego rozwoju biometrycznych systemów bezpieczeństwa[91],
- przeznaczenie 85 mln euro na projekty bezpieczeństwa online w ramach programu *Horizon 2020*[92],
- przegłosowanie przez Parlament Europejski dyrektywy dotyczącej bezpieczeństwa informacji i sieci w marcu 2014 roku (*Great news*, 2014),
- rozpoczęcie w styczniu 2014 roku finansowanego przez UE projektu *PANOPTESEC*, którego celem było wykrywanie luk w zabezpieczeniach oraz reagowanie na cyberataki[93],
- opublikowanie w październiku 2013 roku przez ENISA podręcznika poświęconego ochronie systemów kontroli przemysłowej (ICS) (*Good practice*, 2013).

Reasumując, można się pokusić o kilka wniosków na temat charakteru polityki cyberbezpieczeństwa Unii Europejskiej. Bruksela powieliła tendencje widoczne w innych organizacjach międzynarodowych, takich jak NATO czy ONZ. Co prawda pierwsze ruchy na tym polu UE poczyniła jeszcze w latach 90. XX wieku, uświadomienie sobie wagi zagrożeń w cyberprzestrzeni nastąpiło jednak dopiero po 2007 roku. Należy ponadto zwrócić uwagę, iż początkowo prace w tej dziedzinie toczyły się bardzo powoli, a kolejne inicjatywy Komisji Europejskiej nie przynosiły oczekiwanych rezultatów. Mimo bogactwa dokumentów, strategii, komunikatów i raportów w praktyce kooperacja krajów europejskich dotycząca bezpieczeństwa sieci i informacji była bardzo ograniczona. Rzeczywisty przełom nastąpił dopiero w 2013 roku, kiedy przyjęto strategię cyberbezpieczeństwa zawierającą szereg posiadających fundamentalne znaczenie zapisów. Nie dość, że zrezygnowano wówczas z bardzo wąskiego spojrzenia na problematykę zagrożeń teleinformatycznych, to jeszcze zaryzykowano wprowadzenie klauzuli solidarności. Tak kompleksowe podejście pozornie mogło świadczyć o chęci rywalizacji z NATO, lecz w rzeczywistości zastrzeżono, że UE będzie współpracować z Paktem, tak aby nie powielać jego kompetencji.

[91] *Tabula Rasa project to take biometric security systems to the next level*. European Commission, 22.10.2013: http://ec.europa.eu/digital-agenda/en/news/tabula-rasa-project-take-biometric-security-systems-next-level; dostęp: 21.03.2014.

[92] *85 milion EU cash for online safety projects; six projects already helping to keep you safe online*. European Commission, 28.02.2014: http://ec.europa.eu/digital-agenda/en/news/%E2%82%AC85-million-eu-cash-online-safety-projects-six-projects-already-helping-keep-you-safe-online; dostęp: 21.03.2014.

[93] *PANOPTESEC — Launch of EU-funded Cyber Security Project to handle security incidents*. European Commission, 23.01.2014: http://ec.europa.eu/digital-agenda/en/news/panoptesec-launch-eu-funded-cyber-security-project-handle-security-incidents; dostęp: 21.03.2014.

W tym kontekście można jednak zaryzykować stwierdzenie, iż mimo wartościowych rozwiązań polityczno-prawnych Unia Europejska nie zdołała na początku drugiej dekady XXI wieku wypracować skutecznych mechanizmów praktycznej współpracy państw członkowskich w tej dziedzinie. Podniesienie wydatków na ten cel czy takie przedsięwzięcia, jak utworzenie EC3, były krokiem w dobrą stronę, lecz nie można ich porównywać pod względem przydatności i skuteczności do takich inicjatyw, jak ITU-IMPACT czy CCD COE.

5.5. Rada Europy wobec zjawiska cyberprzestępczości

Oprócz omówionych wyżej mechanizmów współpracy wypracowanych przez ONZ, ITU, NATO i UE dla zobrazowania ogólnoświatowych tendencji można wskazać na jeszcze kilka innych, zróżnicowanych inicjatyw o nieco mniejszej skali, których celem jest podniesienie poziomu bezpieczeństwa teleinformatycznego. Warto zwrócić uwagę na starania podejmowane przez Radę Europy, która problematyką tą zainteresowała się stosunkowo wcześnie. 23 listopada 2001 roku podpisano w Budapeszcie *Konwencję o cyberprzestępczości*, w której zawarto szereg nowatorskich jak na tamten okres ustaleń i rekomendacji. Jak stwierdził Rafał Tarnogórski (2009: 207), była to pierwsza umowa międzynarodowa, która skupiła się na walce z przestępstwami komputerowymi. Jej podstawowym celem było uzupełnienie obowiązujących dotychczas traktatów, które regulowały m.in. kwestię ekstradycji czy pomocy prawnej w sprawach karnych. Ustaliła podstawowe definicje takich terminów, jak *system informatyczny*, *dane informatyczne*, *dostawca usług*, *dane dotyczące ruchu*. Było to o tyle ważne, iż wpływało na ujednolicenie stosowanej przez sygnatariuszy nomenklatury, co było z reguły sprawą mocno kontrowersyjną. W sposób wyczerpujący scharakteryzowano w niej ponadto 5 typów cyberprzestępczości:

- przestępstwa przeciwko poufności, integralności i dostępności danych i systemów informatycznych (zaliczono do nich takie działania, jak uzyskanie nielegalnego dostępu, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu oraz niewłaściwe użycie urządzeń),
- przestępstwa komputerowe, w tym fałszerstwa oraz oszustwa,
- przestępstwa związane z treścią informacji pojawiających się w sieci, przez co rozumiano zamieszczanie online materiałów z pornografią dziecięcą,
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych,
- pozostałe, w tym usiłowanie, pomocnictwo lub podżeganie.

Konwencja uregulowała również podstawowe zasady i mechanizmy współpracy międzynarodowej w zakresie zwalczania tego procederu, w tym np. procedury związane z wnioskami o udzielenie pomocy prawnej, poufności informacji czy zabezpieczania danych teleinformatycznych[94]. Warto dodać, iż w ramach Rady Europy powstał osobny Komitet ds. *Konwencji o cyberprzestępczości*, który zajmuje się m.in. ułatwianiem implementacji jej zapisów, wymianą informacji, a także wydawaniem opinii na wniosek innych organów RE (*T-CY Rules*, 2013). Na tej podstawie można więc stwierdzić, iż był to pierwszy tak kompleksowy dokument, który w sposób całościowy uregulował kwestię międzynarodowych wysiłków na rzecz zwalczania cyberprzestępczości.

Konwencja o cyberprzestępczości dość szybko wywołała jednak skrajne reakcje i opinie. Z jednej strony traktat spotkał się ze znaczącym zainteresowaniem społeczności międzynarodowej, która dostrzegła jego nowatorski i unikalny charakter. Przede wszystkim, jak wspomniano, zauważyły to niektóre organy Organizacji Narodów Zjednoczonych. Ponadto wsparcie dla regulacji zawartych w tej umowie wyraziło wiele innych organizacji międzynarodowych, w tym Unia Europejska, INTERPOL, Organizacja Państw Amerykańskich czy Współpraca Gospodarcza Azji i Pacyfiku. O popularności konwencji świadczył również fakt, iż do 2014 roku aż 42 państwa, również spoza Europy, zgłosiły do niej akces. Wśród nich znalazły się np. Stany Zjednoczone, Panama, Japonia, Izrael czy Australia. Oprócz nich zapisy traktatu wspierało także wiele podmiotów sektora prywatnego, w szczególności tych, które były zainteresowane wzmocnieniem ochrony praw autorskich. Z drugiej jednak strony dokument ten wywoływał regularnie napięcia na arenie międzynarodowej, które przejawiały się trojako. Do konwencji sceptycznie podchodzili niektórzy dostawcy usług internetowych, którzy obawiali się, że może ona przyczynić się do zwiększenia nacisków ze strony służb związanych z monitorowaniem oraz udzielaniem informacji na temat aktywności użytkowników w Internecie. Na przestarzały charakter tej umowy wskazywali ponadto niektórzy przedstawiciele organizacji międzynarodowych. Z czasem na jeden z głównych ośrodków opozycyjnych wobec niej wyrósł Sekretariat Międzynarodowego Związku Telekomunikacyjnego. W konwencji upatrywano także możliwości zwiększonego dostępu podmiotów zewnętrznych do narodowej cyberprzestrzeni, co oznaczałoby osłabienie kontroli rządów nad znajdującą się w granicach państwa infrastrukturą teleinformatyczną. Jak wspomniano, taką optykę przyjęła Federacja Rosyjska, która od drugiej połowy lat 90. XX wieku naciskała na rozpoczęcie prac nad traktatem regulującym podstawowe zachowania państw w sieci wobec cyberataków. Według Moskwy udostępnianie danych z sieci krajowych oznaczałoby więc

[94] *Konwencja o cyberprzestępczości*. Rada Europy, Budapeszt 23.11.2001: http://nowe technologie.umk.pl/wp-content/uploads/2013/04/Konwencja-o-cyberprzestepczosci.pdf; dostęp: 21.03.2014.

naruszenie narodowej suwerenności. Wszystkie te kontrowersje i wątpliwości doprowadziły do sytuacji, w której aż 11 państw, które podpisało umowę, nie ratyfikowało jej. Wśród nich znalazły się m.in. Polska, Szwecja, Irlandia oraz Grecja[95].

Oprócz konwencji Rada Europy od początku XXI wieku podejmowała szereg innych inicjatyw zmierzających do rozwoju współpracy członków w zakresie bezpieczeństwa teleinformatycznego. Należy tutaj wspomnieć o protokole dodatkowym do konwencji, który został opracowany na przełomie 2002 i 2003 roku i który został podpisany w 2003 roku przez 20 państw, a kilkanaście następnych dołączyło w kolejnych latach. Jak stwierdzono w artykule 1. dokumentu, został on opracowany, aby uzupełnić konwencję w zakresie kryminalizacji aktów ksenofobicznych i rasistowskich przy wykorzystaniu systemów komputerowych. W artykule 2. zdefiniowano „materiały rasistowskie i ksenofobiczne" jako teksty, zdjęcia lub inne środki przekazu, które zawierają pomysły lub teorie promujące nienawiść lub dyskryminację na tle rasowym, koloru skóry, pochodzenia narodowego lub etnicznego, a także wyznawanej religii. W protokole zobowiązano strony do zaktualizowania swojego systemu prawnego w taki sposób, aby karał rozpowszechnianie takich materiałów za pomocą systemów komputerowych, groźby i obelgi o podłożu rasistowskim i ksenofobicznym, a także próby usprawiedliwiania zbrodni przeciwko ludzkości (*Additional protocol to the Convention on Cybercrime*). Z jednej strony protokół ten był więc kontynuacją wielowymiarowych działań, które od dawna podejmowała Rada Europy przeciwko tzw. mowie nienawiści, z drugiej jednak mógł on budzić uzasadnione wątpliwości, ponieważ ze względu na bardzo ogólne zapisy dawał rządom prawo do ograniczania pierwotnych praw i zasad, na których został ufundowany Internet. Potencjalnie mogło to prowadzić do nadmiernej kontroli treści zamieszczanych w sieci przy zastosowaniu autorytatywnej i niejednoznacznej interpretacji. Warto zaznaczyć, iż szereg państw nie zdecydowało się w końcu podpisać tego dokumentu. Wśród sygnatariuszy zabrakło m.in. Stanów Zjednoczonych, Japonii, Izraela, Wielkiej Brytanii, Turcji, Rosji, Irlandii czy Gruzji. Aż 18 państw, które to zrobiło, nie ratyfikowało go później (jak np. Kanada, Szwecja, Hiszpania, Polska, Grecja czy Estonia[96]). Wiele rządów zgłosiło zastrzeżenia wobec niektórych zapisów dokumentu, jak m.in. Chorwacja, Dania, Finlandia

[95] M.A. Vatis: *The Council of Europe Convention on Cybercrime*, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, National Academy of Sciences 2010, s. 218—219: http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf; dostęp: 24.03.2014; *Convention on Cybercrime*. CETS No.: 185, Council of Europe: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG; dostęp: 24.03.2014.

[96] *Additional protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*. CETS No.: 189, Council of Europe: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG; dostęp: 24.03.2014.

oraz Rumunia[97]. Sytuację tę trafnie podsumowała Isabelle Rorive (2009: 422), według której protokół dodatkowy poniósł porażkę, jeśli chodzi o próbę wypracowania międzynarodowych standardów zwalczania „mowy nienawiści".

Bez względu na to fiasko Rada Europy angażowała się w wiele innych przedsięwzięć na polu cyberbezpieczeństwa. Po pierwsze można wspomnieć o wspólnej z Unią Europejską inicjatywie o nazwie GLACY (Global Action on Cybercrime), na którą przeznaczono 3,35 mln euro. Za główny cel tego programu, przewidzianego na lata 2013—2016, uznano rozwój współpracy między organami ścigania w oparciu o zapisy *Konwencji Rady Europy o cyberprzestępczości*. W tym celu przewidziano działania zmierzające m.in. do harmonizacji rozwiązań prawnych państw członkowskich, wspólne szkolenia, wymianę informacji oraz rozwój zdolności podmiotów zajmujących się zwalczaniem cyberprzestępczości. W praktyce jednym z pierwszych, ważniejszych przejawów GLACY była konferencja zorganizowana w Dakarze w dniach 24—27 marca 2014 roku[98].

Po drugie rozpoczęto *Project Cybercrime@Octopus*, który miał trwać od 1 stycznia 2014 do 31 grudnia 2016 roku. Do głównych zadań programu zaliczono organizację corocznych konferencji z serii *Octopus*, wsparcie funkcjonowania Komitetu ds. *Konwencji o cyberprzestępczości*, a także pomoc dla państw, które wyraziły gotowość jej implementacji. W przeciwieństwie do GLACY ten projekt miał jednak bardzo małe znaczenie, głównie ze względu na niewielkie fundusze, oscylujące w granicach 1,8 mln euro[99].

Po trzecie w latach 2011—2013 Rada Europy wraz z Unią Europejską zrealizowały program wpisany w ramy Partnerstwa Wschodniego (Eastern Partnership — Cooperation against Cybercrime, Cyber@EAP). Jego głównym celem była promocja przyjętych dotychczas rozwiązań w zakresie zwalczania cyberprzestępczości w Armenii, Azerbejdżanie, Mołdawii, Białorusi, Gruzji oraz na Ukrainie. Inicjatywa ta przewidywała m.in. podnoszenie świadomości decydentów co do zwalczania przestępczości komputerowej, ocenę przyjętych przez te kraje rozwiązań, wspólne ćwiczenia związane m.in. z pozyskiwaniem dowodów w formie cyfrowej, wzmocnienie kooperacji organów ścigania czy organizację regionalnych konferencji[100].

---

[97] *List of declarations made with respect to treaty No. 189*. Council of Europe: http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=189&CM=8&DF=&CL=ENG&VL=1; dostęp: 24.03.2014.

[98] *Global Action on Cybercrime*. Council of Europe: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/GLACY_en.asp; dostęp: 24.03.2014.

[99] *Project Cybercrime@Octopus*. Council of Europe, 20.02.2014: www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_octo_summary_V10.pdf; dostęp: 24.03.2014.

[100] *Eastern Partnership — Cooperation against Cybercrime (Cyber@EAP)*. Council of Europe, European Union: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_eap_cyber_summary1_%2818_June_12%29.pdf; dostęp: 24.03.2014.

Po czwarte podobny projekt (*Regional Cooperation against Cybercrime in South-Eastern Europe*) realizowano w latach 2010—2013 na Bałkanach. Ufundowany przez Komisję Europejską, a nadzorowany przez Radę Europy, objął m.in. Albanię, Bośnię i Hercegowinę, Chorwację, Serbię oraz Turcję. Głównym jego założeniem było wzmocnienie zdolności państw tego regionu do współpracy w zakresie zwalczania przestępczości komputerowej poprzez takie działania, jak harmonizacja systemów prawnych, wspólne szkolenia, kontakty z dostawcami usług internetowych lub opracowanie strategii i polityk zwalczania cyberprzestępczości. Na program przeznaczono ok. 2,7 mln euro. Wsparły go ponadto Francja, Włochy, Słowenia oraz Rumunia[101].

Po piąte w latach 2006—2009 przeprowadzono *Project against Cybercrime*, który w zamyśle miał wspierać proces przyjmowania na całym świecie *Konwencji o cyberprzestępczości* Rady Europy. Przeznaczono na niego w sumie ok. 1,1 mln euro, które wykorzystano nie tylko na promocję samego dokumentu, ale również na aktualizację systemów prawnych zgodnie z jego zapisami, podnoszenie zdolności organów ścigania w tym zakresie, a także na intensyfikację współpracy międzynarodowej. W praktyce w ramach programu zorganizowano szereg konferencji i spotkań poświęconych przestępczości komputerowej lub wzięto w takowych udział. Można tu wymienić np. regionalną konferencję w Belgradzie w marcu 2007 roku, warsztaty dla prokuratorów w São Paulo we wrześniu 2007 roku, konferencję we Francji w czerwcu 2008 roku czy warsztaty w Buenos Aires w lipcu 2008 roku[102]. Druga faza tego projektu, na którą przeznaczono 1,4 mln euro, została przeprowadzona w latach 2009—2011. W jego ramach zainteresowano się również takimi zagadnieniami, jak ochrona dzieci online, ochrona danych oraz prywatności czy szkolenia dla sędziów i prokuratorów. Warto dodać, iż program został wsparty finansowo przez Estonię, Japonię, Monako, Rumunię, a także korporacje Microsoft oraz McAfee[103].

Można także wspomnieć o unikalnym projekcie poświęconym zwalczaniu cyberprzestępczości w Gruzji zrealizowanym w latach 2009—2010 przez Komisję Europejską, Radę Europy oraz rząd tego kraju, na który przeznaczono sumę 220 000 euro. Głównym powodem zainicjowania tego programu była wojna gruzińsko-rosyjska z sierpnia 2008 roku, w związku z tym podstawowym założeniem projektu było wzmocnienie bezpieczeństwa teleinformatycznego Gruzji,

[101] *Regional Cooperation against Cybercrime in South-Eastern Europe*. Council of Europe, European Union, 08.02.2013: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Project_Summary_%28Cybercrime_IPA%29_dec_12.pdf; dostęp: 24.03.2014.

[102] *Project on Cybercrime. Summary and Workplan 2008—2009*. Council of Europe, 14.08.2008: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-summary_workplan2008-2009c_14aug08.pdf; dostęp: 24.03.2014.

[103] *Global Project on Cybercrime (Phase 2)*. Council of Europe, 26.09.2011: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/2079%20adm%20pro%20summary%20_26%20Sep%202011_.pdf; dostęp: 24.03.2014.

jak również wykształcenie przez nią spójnej strategii zwalczania cyberzagrożeń. Skonkretyzowano go w czterech celach. Po pierwsze Rada Europy miała wesprzeć Tbilisi w pracach nad dostosowaniem własnego systemu prawnego do założeń *Konwencji o cyberprzestępczości*. Po drugie przewidziano prowadzenie działań szkoleniowych. Po trzecie podkreślono potrzebę budowania nowych struktur ułatwiających zwalczanie przestępczości komputerowej oraz współpracę międzynarodową (np. wyspecjalizowanych jednostek policji). Po czwarte projekt miał wspierać współpracę na linii organy ścigania — dostawcy usług internetowych[104].

Wszystkie powyższe dane pozwalają stwierdzić, iż Rada Europy stała się na początku XXI wieku jedną z aktywniejszych organizacji regionalnych na polu cyberbezpieczeństwa. Najbardziej doniosłym przejawem jej prac stała się oczywiście *Konwencja o cyberprzestępczości* z 2001 roku, która szczególnie w pierwszej dekadzie XXI wieku była dokumentem nowatorskim i bardzo ważnym dla praktycznej współpracy państw w przestrzeni teleinformatycznej. Pozwoliła ona wypracować pewne podstawowe zasady kooperacji organów ścigania sygnatariuszy, a także wywarła trudny do przecenienia wpływ w wymiarze koncepcyjnym na prace innych organizacji międzynarodowych. Jednocześnie jednak można się zgodzić z opinią, iż w ciągu kilkunastu lat uległa ona częściowej dezaktualizacji, zarówno ze względu na wielokrotny wzrost skali, jak i częściową zmianę charakteru zagrożeń komputerowych, zasadne wydają się zatem głosy wskazujące na potrzebę modyfikacji tego dokumentu lub opracowania nowego, przystającego do wyzwań połowy drugiej dekady XXI wieku. Jest to tym bardziej ewidentne, iż *Konwencja o cyberprzestępczości* wywoływała skrajne reakcje w środowisku międzynarodowym. Wątpliwości budził również protokół dodatkowy, który spotkał się ze zdecydowanie mniejszym zainteresowaniem państw członkowskich. Rada Europy nie wykazywała jednak takich zamiarów, skupiając się w realizowanych przez siebie programach właśnie na promocji traktatu z 2001 roku. Zarówno ze względu na ograniczone fundusze, jak i zakres tych przedsięwzięć, ich bezpośrednie efekty okazały się znikome.

Reasumując ten wątek, można stwierdzić, iż Rada Europy w wymiarze koncepcyjnym odegrała istotną rolę w międzynarodowej debacie poświęconej zwalczaniu cyberprzestępczości, choć jej działalność wywoływała wiele napięć i kontrowersji osłabiających efektywność podejmowanych przez nią przedsięwzięć.

[104] *Project on Cybercrime in Georgia*. Council of Europe, European Union: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215%20adm%20pro%20summary.pdf; dostęp: 24.03.2014.

5.6. Szanghajska Organizacja Współpracy jako narzędzie polityki cyberbezpieczeństwa Chin i Rosji

Kolejną organizacją regionalną, która zainteresowała się problematyką bezpieczeństwa teleinformatycznego, była Szanghajska Organizacja Współpracy, której członkami są Rosja, Chiny, Kazachstan, Kirgistan, Tadżykistan i Uzbekistan, członkami obserwatorami SCO zostały natomiast Afganistan, Pakistan, Indie, Mongolia oraz Iran. Deklaracja o utworzeniu organizacji z 2001 roku wyznaczyła jej bardzo szerokie kompetencje, wśród których wymieniono pogłębianie zaufania oraz dobrosąsiedzkiej przyjaźni, wspieranie współpracy członków w wymiarze politycznym, gospodarczym, handlowym, naukowym, technologicznym, kulturowym, edukacyjnym, komunikacyjnym i innych, współpracę w zakresie ochrony regionalnego pokoju, bezpieczeństwa i stabilności, a także ustanowienie demokratycznego, sprawiedliwego i racjonalnego międzynarodowego porządku politycznego i gospodarczego (*Declaration on the Establishment*, 2001). Tak szerokie uprawnienia, jak również interesujący skład członkowski, sprawiły, iż od początku XXI wieku SCO zaczęła odgrywać rosnącą rolę w stosunkach międzynarodowych na obszarze Azji. Zrzeszając dwie potęgi atomowe, jak również blisko współpracując z kluczowymi graczami w regionie (Indie, Pakistan, Afganistan, Iran), struktura ta zaczęła być postrzegana jako istotny element globalnego środowiska bezpieczeństwa. Część badaczy uznała ją wręcz za rodzący się sojusz wojskowy, porównywalny z Paktem Północnoatlantyckim. Marcel de Haas oraz Frans-Paul van der Putten (2007: 57) za główną różnicę między nimi uznali fakt, iż SCO skupiała się przede wszystkim na bezpieczeństwie na obszarze państw członkowskich, podczas gdy Sojusz działał także w wymiarze zewnętrznym. O rosnącym nacisku na tę problematykę świadczyły decyzje i deklaracje przyjęte przez Szanghajską Organizację Współpracy po 2001 roku. Należy tu wymienić m.in. *Konwencję o zwalczaniu terroryzmu, separatyzmu i ekstremizmu* z 15 czerwca 2001 roku czy porozumienia o współpracy antyterrorystycznej z 2004 i 2007 roku[105]. Na takie tendencje wskazywało również zacieśnianie współpracy wojskowej krajów SCO, czego wyrazem były m.in. wspólne manewry wojskowe przeprowadzone np. w sierpniu 2005 roku czy sierpniu 2007 roku (de Haas, 2007: 248).

Procesy te doprowadziły naturalnie do wzrostu zainteresowania Szanghajskiej Organizacji Współpracy wyzwaniami dla bezpieczeństwa teleinformatycznego. Było to tym bardziej ewidentne, iż jej członkami były Rosja i Chiny należące, jak wiadomo, do ścisłej czołówki krajów najaktywniej działających w cyber-

[105] *Key Normative Documents of the Shanghai Cooperation Organisation*. Human Rights in China: www.hrichina.org/sites/default/files/PDFs/Reports/SCO/2011-HRIC-SCO-Whitepaper-AppendixA-SCO-Docs.pdf; dostęp: 26.03.2014.

przestrzeni. Ponadto, jak wspomniano, SCO współpracowała m.in. z Iranem, Pakistanem i Indiami, które miały poważne problemy na tym tle[106]. W związku z tym organizacja stosunkowo szybko podjęła działania, których celem było zawiązanie współpracy na obszarze cyberbezpieczeństwa. Po raz pierwszy szerzej zainteresowano się tą problematyką w sierpniu 2007 roku na spotkaniu głów państw SCO w Biszkeku. Przyjęto wówczas plan działań w zakresie „międzynarodowego bezpieczeństwa informacyjnego" (*international information security*). Zapowiedziano w nim, że w obliczu rosnących wyzwań teleinformatycznych rządy będą współpracowały, aby im skutecznie przeciwdziałać[107]. Temat ten podjęto również w 2008 roku, kiedy głowy krajów członkowskich spotkały się w Duszanbe. We wspólnym komunikacie podkreślono zasadnicze znaczenie rezolucji Zgromadzenia Ogólnego ONZ nr 62/17 na temat bezpieczeństwa teleinformatycznego, zapowiadając wsparcie jej wdrażania. Przywódcy zapowiedzieli także stworzenie międzyrządowego porozumienia w ramach Szanghajskiej Organizacji Współpracy w dziedzinie bezpieczeństwa informacyjnego (*Dushanbe Declaration*, 2008).

W czerwcu 2009 roku na kolejnym szczycie SCO w Jekaterynburgu po raz kolejny poruszono ten problem. W deklaracji końcowej uznano bezpieczeństwo informacyjne za jeden z „kluczowych elementów" międzynarodowego systemu bezpieczeństwa (*Yekaterinburg Declaration*, 2009). Na spotkaniu roboczym w październiku tego roku w Pekinie zapowiedziano natomiast stworzenie „superinfostrady" (*SCO information superhighway*) (*Joint Communiqué*, 2009). W 2009 roku Federacja Rosyjska zaproponowała podpisanie umowy poświęconej „współpracy w dziedzinie międzynarodowego bezpieczeństwa informacyjnego". W artykule 2. tego dokumentu wymieniono główne cyberzagrożenia dla państw członkowskich, takie jak rozwój i wykorzystanie broni informacyjnych, przygotowanie oraz prowadzenie wojen informacyjnych, terroryzm informacyjny, przestępczość informacyjna, wykorzystanie dominującej pozycji w środowisku informacyjnym do wyrządzania szkód innym państwom, rozpowszechnianie informacji szkodliwych dla systemów politycznych, gospodarczych i społecznych innych krajów (w tym takich kwestii, jak moralność czy kultura), a także naturalne lub stworzone przez człowieka zagrożenia prawidłowego funkcjonowania elementów narodowych infrastruktur informacyjnych.

W artykule 3. uzgodniono główne obszary współpracy państw w tej dziedzinie. Wymieniono tu m.in. identyfikację oraz wdrożenie wspólnych instrumentów zapewniania bezpieczeństwa informacyjnego, wdrożenie systemu monitorowania i wspólnego reagowania na zagrożenia, opracowanie środków rozwoju

[106] Z jednej strony chodziło tu o omówione już incydenty związane np. z robakiem *Stuxnet*, z drugiej natomiast o regularny konflikt toczący się w cyberprzestrzeni między grupami haktywistycznymi Pakistanu i Indii. Zob. Kshetri, 2005: 551.

[107] *Global Strategic Report*. International Telecommunication Union: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapt_1_iframe.htm; dostęp: 26.03.2014.

norm prawa międzynarodowego, które powstrzymałyby proliferację broni informacyjnych, zapobieganie wykorzystaniu ICT przez terrorystów, zapobieganie cyberprzestępczości, prowadzenie wspólnych badań, wspieranie stabilnego funkcjonowania oraz internacjonalizacji globalnego zarządzania Internetem, zabezpieczanie infrastruktury krytycznej państw członkowskich, interakcję z innymi podmiotami międzynarodowymi oraz wymianę informacji.

Ponadto w dwóch aneksach zawarto nie tylko definicje podstawowych terminów, lecz również dokładną charakterystykę głównych zagrożeń. W aneksie 1. zdefiniowano przede wszystkim *wojnę informacyjną*, którą uznano za

> konfrontację między dwoma lub więcej państwami w przestrzeni informacyjnej, której celem jest uszkodzenie systemów, procesów i zasobów informacyjnych, krytycznych oraz innych struktur [dla — M.L.] podkopania politycznych, ekonomicznych i społecznych systemów, masowego, psychologicznego prania mózgów w celu destabilizacji społeczeństwa i państwa, jak również zmuszenia do podjęcia decyzji leżących w interesie przeciwnej strony.

Znalazły się tam również definicje takich pojęć, jak *broń informacyjna*, *przestrzeń informacyjna*, *zasoby informacyjne*, *terroryzm informacyjny* czy *międzynarodowe bezpieczeństwo informacyjne*. W aneksie 2. natomiast omówiono podstawowe zagrożenia w tej dziedzinie. Charakteryzując wojnę informacyjną, wspomniano, iż rozwój broni informacyjnych może prowadzić do nowego wyścigu zbrojeń. Za obszary szczególnie zagrożone tego typu działaniami uznano m.in. systemy transportowe, komunikacyjne, kontroli lotów, obronę przeciwrakietową, a także inne zdolności obronne, co mogłoby doprowadzić w konsekwencji do utraty legalnego prawa do samoobrony. Za interesujący należy również uznać punkt 5. dotyczący rozpowszechniania szkodliwych dla systemów politycznych, gospodarczych i społecznych informacji. Stwierdzono tam, iż może się to przejawiać powtarzalnym pojawianiem się w mediach cyfrowych wiadomości, które zakłócają percepcję m.in. systemu politycznego, społecznego, polityki wewnętrznej czy międzynarodowej, jednocześnie promując idee terrorystyczne, separatystyczne lub ekstremistyczne, zmierzające do pojawienia się konfliktów międzyetnicznych, międzyrasowych czy międzyreligijnych[108].

Projekt umowy należy uznać za niezwykle interesujący i nowatorski, jako jeden z pierwszych zawierał bowiem nie tylko zobowiązanie do pogłębiania współpracy w zakresie bezpieczeństwa teleinformatycznego, ale także wyraźne definicje większości podstawowych typów cyberzagrożeń oraz najważniejszych terminów. Inną jego unikalną cechą było zastosowanie pojęć wywodzących się ze scharakteryzowanej już szerokiej kategorii informacji. Jak wspomniano

[108] Tłumaczenie nieoficjalne. Zob. *Agreement between the Governments*, 2009. Za: Boland, 2011, s. 13; Kanuck, 2009: 1575.

wcześniej, Rosja i Chiny nie zgadzały się z amerykańskim stanowiskiem, które akcentowało wagę zachowania wolności słowa w sieci. Moskwa i Pekin postrzegały natomiast aktywność w Internecie, szczególnie w kontekście „kolorowych" rewolucji, jako potencjalne zagrożenie dla swojej stabilności wewnętrznej. Stąd wynikały zapisy, które skupiały się nie tylko na samych cyberatakach i sposobach obrony przed nimi, ale również na zagadnieniu działań psychologicznych, propagandowych online. Można się więc tutaj zgodzić z Abrahamem D. Sofaerem, Davidem Clarkiem oraz Whitfieldem Diffiem (2010: 186), którzy zauważyli, iż SCO starało się potwierdzić w swojej polityce prawo do kontroli państw nad narodowymi elementami cyberprzestrzeni.

W kolejnych latach ten kierunek prac organizacji był kontynuowany. W kwietniu 2010 roku przyjęto wspólną deklarację Szanghajskiej Organizacji Współpracy oraz Sekretariatu Organizacji Narodów Zjednoczonych, w której zapowiedziano pogłębienie współpracy w zwalczaniu zagrożeń dla bezpieczeństwa międzynarodowego. Co prawda nie wyszczególniono tu wyraźnie wyzwań pojawiających się w cyberprzestrzeni, lecz wspomniano m.in. o terroryzmie czy transnarodowej przestępczości (*Joint Declaration on SCO*/*UN*, 2010). Ważne stwierdzenie znalazło się ponadto w deklaracji końcowej szczytu SCO zorganizowanego w Taszkiencie w czerwcu 2010 roku. Podkreślono w nim, że bezpieczeństwo informacyjne „jest blisko związane z zapewnieniem suwerenności państwowej, bezpieczeństwa narodowego, społecznej i ekonomicznej stabilności oraz interesów obywateli". Zaakcentowano, iż każdy kraj ma prawo regulować Internet, pogłębiając zarazem współpracę międzynarodową w duchu równouprawnienia i wzajemnego szacunku. Zauważono także, iż technologie teleinformatyczne powinny być wykorzystywane wyłącznie w celach pokojowych, i zapowiedziano dalsze działania zmierzające do zapewnienia „międzynarodowego bezpieczeństwa informacyjnego" (*Declaration of the Tenth Meeting*, 2010).

Kolejne ważne deklaracje miały miejsce na szczycie Szanghajskiej Organizacji Współpracy w Astanie w czerwcu 2011 roku. W komunikacie głów państw stwierdzono, iż biorąc pod uwagę narastające wyzwania teleinformatyczne, strony będą działały na rzecz określenia podstawowych norm postępowania w tym środowisku (*Joint Communiqué of meeting*, 2011). Wyrazem tego był m.in. omówiony już list Rosji i Chin do sekretarza generalnego ONZ z września 2011 roku (*Letter dated 12 September 2011*, 2011). Warto również wspomnieć o przyjętej na tym samym spotkaniu deklaracji związanej z 10. rocznicą funkcjonowania organizacji. W punkcie VII. stwierdzono, iż rosnąca skala cyberprzestępczości wymaga intensywnej współpracy międzynarodowej, w związku z czym zadeklarowano gotowość SCO do współdziałania z innymi aktorami stosunków międzynarodowych (*Astana Declaration*, 2011). Zainteresowanie problematyką cyberzagrożeń było widoczne w pracach Szanghajskiej Organizacji Współpracy także w kolejnych latach. W 2012 roku na spotkaniu głów państw

uzupełniono priorytety SCO co do zwalczania „terroryzmu, separatyzmu i ekstremizmu" o międzynarodową cyberprzestępczość[109], natomiast we wrześniu 2013 roku w deklaracji przyjętej w Biszkeku zauważono rosnącą rolę Internetu jako środka rozpowszechniania treści ekstremistycznych oraz rekrutacji przez organizacje terrorystyczne. W tym kontekście wyrażono więc chęć pogłębienia współpracy między krajowymi agencjami zajmującymi się bezpieczeństwem teleinformatycznym[110].

Powyższe dokumenty i deklaracje niestety tylko w niewielkim stopniu przekładały się na rozwój mechanizmów bezpośredniej, praktycznej kooperacji państw członkowskich. Kontakty w tej dziedzinie były utrzymywane głównie poprzez Regionalną Strukturę Antyterrorystyczną (Regional Anti-Terrorism Structure) SCO, która pełniła przede wszystkim funkcje koordynacyjne oraz naukowo-badawcze, przygotowując np. wspólne szkolenia, manewry czy analizy dotyczące bieżącej sytuacji bezpieczeństwa w Azji. Należy podkreślić, iż stosunkowo późno i w bardzo ograniczonym stopniu zainteresowała się ona problematyką cyberzagrożeń[111].

Powyższe rozważania pozwalają sformułować kilka wniosków na temat polityki cyberbezpieczeństwa Szanghajskiej Organizacji Współpracy. Przede wszystkim, podobnie jak w przypadku NATO, zainteresowała się ona na większą skalę zagrożeniami teleinformatycznymi dopiero po wydarzeniach w Estonii w 2007 roku. SCO przyjęła specyficzną i odmienną od zachodniej strategię działania w tej dziedzinie, skupiła się bowiem na szerokiej i wieloznacznej kategorii bezpieczeństwa informacyjnego, akcentując nie tylko wyzwania związane z samymi włamaniami komputerowymi, lecz także z działalnością propagandową online. Można zatem zaryzykować stwierdzenie, iż Szanghajska Organizacja Współpracy służyła Federacji Rosyjskiej oraz Chińskiej Republice Ludowej jako jeden z instrumentów promocji własnej wizji współpracy międzynarodowej na polu cyberbezpieczeństwa, ponieważ w dokumentach organizacji wielokrotnie akcentowano prawo rządów do kontrolowania własnych sieci komputerowych, co leżało w interesie zarówno Moskwy, jak i Pekinu. W wymiarze koncepcyjnym rozwiązania przyjmowane lub promowane przez organizację były bogate w treści i nowatorskie, o czym świadczyła w szczególności rosyjska inicjatywa z 2009 roku. Niestety nie przełożyły się one na wypracowanie mechani-

[109] *The Shanghai Cooperation Organisation (SCO)*. CyberCrime Law, 2012: www.cybercrimelaw.net/SCO.html; dostęp: 26.03.2014.

[110] J. Famularo: *The Latest from the Shanghai Cooperation Organisation*. „The National Interest" 24.09.2013: http://nationalinterest.org/commentary/the-latest-the-shanghai-cooperation-organization-9118; dostęp: 26.03.2014.

[111] *The Regional Anti-Terrorist Structure of Shanghai Cooperation Organisation*. RATS SCO: http://ecrats.org/en; dostęp: 26.03.2014; *SCO members to cooperate in war on cyber terrorism*, Russia & India Report, 02.04.2013: http://in.rbth.com/world/2013/04/02/sco_members_to_cooperate_in_war_on_cyber_terrorism_23429.html; dostęp: 26.03.2014.

zmów praktycznej współpracy w tej dziedzinie, które byłyby porównywalne nie tylko z NATO, lecz nawet z Radą Europy.

5.7. Polityka bezpieczeństwa teleinformatycznego Współpracy Gospodarczej Azji i Pacyfiku (APEC)

Na kontynencie azjatyckim interesującą strategię cyberbezpieczeństwa opracowała również powstała w 1989 roku Współpraca Gospodarcza Azji i Pacyfiku (APEC). Było to o tyle interesujące, iż z pozoru nie była ona organizacją właściwą do walki z zagrożeniami teleinformatycznymi, ponieważ do jej głównych zadań zalicza się wspieranie trwałego wzrostu gospodarczego oraz dobrobytu[112]. Niemniej struktura ta stosunkowo szybko zaczęła interesować się tymi zagadnieniami, co przede wszystkim wynikało ze świadomości, iż szkodliwe zastosowanie ICT może mieć wymierny wpływ na sytuację ekonomiczną oraz jakość życia społeczeństw. Wpływ na to miał ponadto unikalny skład członkowski[113].

W latach 90. XX wieku organizacja nie podejmowała poważniejszych inicjatyw skupionych wyłącznie na kwestiach bezpieczeństwa teleinformatycznego. Co prawda na spotkaniach ministrów telekomunikacji APEC omawiano czasami te kwestie, czyniono to jednak w sposób bardzo ogólnikowy i nieskonkretyzowany. Zdecydowanie większą uwagę przykładano natomiast do takich kwestii, jak upowszechnienie dostępu do Internetu czy rozwój handlu elektronicznego (zob. *The Third APEC*, 1998; *Annex A*, 1998; *Annex C*, 2000). Zmieniło się to w 2002 roku, kiedy tematykę tę podjęto na szczycie zorganizowanym w Szanghaju. W wydanej tam deklaracji państwa członkowskie stwierdziły, iż APEC będzie działać na rzecz zapewnienia bezpieczeństwa informacji i sieci. Decyzja ta wynikała głównie ze świadomości rosnącej skali zagrożeń dla funkcjonalności infrastruktury teleinformatycznej w całym regionie. W związku z tym ministrowie przyjęli dwa dokumenty (*The Fifth APEC*, 2002): oświadczenie w sprawie bezpieczeństwa infrastruktur informacyjnych i komunikacyjnych (*Statement on the Security of Information and Communications Infrastructures*) oraz plan działań. W pierwszym z nich, odwołując się m.in. do dorobku Rady Europy, zgodzili się na implementację rezolucji Zgromadzenia Ogólnego

[112] *Mission Statement*. APEC: www.apec.org/About-Us/About-APEC/Mission-Statement.aspx; dostęp: 28.03.2014.

[113] W skład APEC wchodzą liderzy w zakresie potencjału do działań w cyberprzestrzeni, w tym np. Stany Zjednoczone, Rosja, Chiny, Korea Południowa. W sumie APEC składa się z 21 państw. Zob. *Member Economies*. APEC: www.apec.org/About-Us/About-APEC/Member-Economies.aspx; dostęp: 28.03.2014.

ONZ nr 55/66. Ponadto zlecono Grupie Roboczej Telekomunikacji i Informacji (APEC Telecommunications and Information Working Group — TEL) uznanie tych zagadnień za priorytet oraz ułatwienie współpracy państw APEC w zakresie ochrony infrastruktury teleinformatycznej. Stwierdzono także potrzebę podjęcia następujących działań: ustanowienia podstaw prawnych zwalczania cyberprzestępczości, rozwoju partnerstwa między sektorem publicznym i prywatnym, stworzenia zespołów reagowania na incydenty komputerowe we wszystkich krajach członkowskich, wymiany informacji między nimi, podnoszenia świadomości użytkowników czy utworzenia zestawu standardów i dobrych praktyk (*Annex B*, 2002). O wiele bardziej interesujący okazał się plan działań, w którym wyznaczono szereg zadań dla polityki cyberbezpieczeństwa APEC. Należy tu wymienić m.in. promocję bezpiecznych i zaawansowanych urządzeń teleinformatycznych, prowadzenie prac badawczych, dobrowolną wymianę technologii, zintensyfikowanie prac Grupy Roboczej Telekomunikacji i Informacji, szczególnie jeśli chodzi o technologie elektronicznego podpisu i identyfikacji oraz rozwój zasobów ludzkich poprzez kooperację pomiędzy rządami oraz pomiędzy rządami i sektorem prywatnym (*Annex A*, 2002).

Zapisy te zostały rozwinięte na kolejnych szczytach Współpracy Gospodarczej Azji i Pacyfiku. W 2005 roku na spotkaniu ministerialnym w Limie przyjęto np. deklarację, która w punkcie 31. podkreśliła wagę prac Grupy Roboczej w zakresie zwalczania przestępczości komputerowej. W punkcie 32. wezwano państwa członkowskie do przestudiowania *Konwencji Rady Europy o cyberprzestępczości* oraz przyjęcia rozwiązań prawnych, które byłyby z nią zgodne. Zdecydowano również o kontynuacji przedsięwzięć w tej dziedzinie, przede wszystkim jeśli chodzi o kooperację narodowych zespołów CERT, walkę z cyberprzestępczością oraz ochronę infrastruktury krytycznej. Wyrażono ponadto zamiar nawiązania bliższych kontaktów z innymi organizacjami, w tym np. z Międzynarodowym Związkiem Telekomunikacyjnym czy Stowarzyszeniem Narodów Azji Południowo-Wschodniej (ASEAN) (*The Sixth APEC*, 2005). Na tym samym spotkaniu przyjęto także program walki ze spamem (*Annex E*, 2005) oraz plan działań dla Grupy Roboczej Telekomunikacji i Informacji. Wyznaczono tam 5 obszarów funkcjonowania TEL: rozwój infrastruktury teleinformatycznej, rozwój polityki i regulacji w tej dziedzinie, podnoszenie poziomu bezpieczeństwa teleinformatycznego, rozwój społeczeństwa informacyjnego oraz wykorzystanie technologii ICT do reagowania na katastrofy naturalne. W obszarze trzecim, dotyczącym bezpieczeństwa, wymieniono następujące cele i inicjatywy: wzmacnianie zdolności krajów APEC do reagowania na incydenty komputerowe, prowadzenie ćwiczeń przez zespoły CERT i CSIRT, walka z cyberprzestępczością, analiza konsekwencji wprowadzania najnowszych, wschodzących technologii, rozwój zestawu wskazówek dotyczących bezpieczeństwa teleinformatycznego dla państw członkowskich czy kooperacja z innymi organizacjami międzynarodowymi (*Annex A*, 2005).

O rosnącej randze tych spraw w pracach APEC świadczyły również deklaracje przyjęte na spotkaniach ministrów telekomunikacji w Bangkoku w kwietniu 2008 roku, na Okinawie w październiku 2010 roku oraz w Sankt Petersburgu w sierpniu 2012 roku. Na pierwszym z tych szczytów przyznano, iż cyberbezpieczeństwo stało się problemem globalnym, wymaga zatem współpracy między państwami, służbami bezpieczeństwa, sektorem biznesowym, przedstawicielami przemysłu oraz samymi użytkownikami. W deklaracji potwierdzono też potrzebę pogłębionych kontaktów między zespołami CERT, kooperacji z innymi organizacjami międzynarodowymi (OECD) czy wprowadzania w poszczególnych krajach rozwiązań prawnych, które opierałyby się na m.in. na rezolucjach Zgromadzenia Ogólnego ONZ oraz *Konwencji Rady Europy o cyberprzestępczości* (*The Seventh APEC*, 2008). Na Okinawie w 2010 roku zwrócono z kolei uwagę na rosnące uzależnienie poszczególnych społeczeństw od technologii ICT, czego skutkiem jest ich większa podatność na cyberzagrożenia. Nowością było przyjęcie do wiadomości oraz poparcie inicjatywy Grupy Roboczej dotyczącej Dnia Świadomości Cyberbezpieczeństwa (*APEC Cybersecurity Awareness Day*). Zauważono ponadto potrzebę ochrony najmłodszych w środowisku teleinformatycznym, m.in. przy współpracy z OECD (*The Eight APEC*, 2010). Na spotkaniu w Sankt Petersburgu w 2012 roku w zasadzie powtórzono wcześniejsze ustalenia z Bangkoku oraz Okinawy. Za główną strukturę odpowiedzialną za politykę cyberbezpieczeństwa uznano wówczas również Grupę Roboczą Telekomunikacji i Informacji (*Saint Petersburg Declaration*, 2012).

Na tej podstawie warto szerzej prześledzić funkcjonowanie tego organu, który został utworzony już w 1990 roku. Początkowo TEL miała za zadanie jedynie ułatwić i przyspieszyć rozwój infrastruktury teleinformatycznej w regionie. Wspominano także o chęci budowy społeczeństwa informacyjnego[114]. Z czasem jednak, na co wskazywały omówione wyżej dokumenty, Grupa Robocza zaczęła coraz bardziej angażować się w inicjatywy dotyczące *stricte* cyberbezpieczeństwa. W 2006 roku dostosowano do tych funkcji jej strukturę, wyodrębniając trzy grupy sterujące. Jedną z nich była Grupa Sterująca ds. Bezpieczeństwa i Dobrobytu (Security and Prosperity Steering Group)[115]. Do jej głównych funkcji zaliczono promocję bezpieczeństwa i zaufania w sieci, współpracę z zespołami reagowania na incydenty komputerowe, walkę ze spamem i oprogramowaniem szpiegowskim, prewencję aktów cyberprzestępczości, rozwój

[114] *Telecommunications and Information*. APEC: http://apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx; dostęp: 28.03.2014.

[115] S.J. Shafie: *APEC TEL. Regional Workshop on Frameworks for Cyber Security and Critical Information Infrastructure Protection*. Asia-Pacific Economic Cooperation, International Telecommunication Union, Hanoi 2007: www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/APECTEL-hanoi-31-august-07.pdf; dostęp: 28.03.2014.

zasobów ludzkich, podnoszenie świadomości użytkowników oraz prowadzenie dialogu z sektorem prywatnym[116]. W praktyce funkcjonowanie TEL opierało się na organizowanych co pół roku spotkaniach, na których prowadzono dyskusje poświęcone cyberbezpieczeństwu państw członkowskich. W ich trakcie szczególną rolę odgrywała Grupa Sterująca (SPSG), która przedstawiała raporty o podejmowanych przez siebie inicjatywach i projektach (Portnoy, Goodman, 2009: 48—50).

Warto zauważyć, iż w przeciwieństwie np. do Szanghajskiej Organizacji Współpracy APEC rzeczywiście starała się realizować w praktyce przyjęte przez siebie założenia. Od połowy pierwszej dekady XXI wieku Grupa Robocza zrealizowała wiele interesujących inicjatyw, do których należy zaliczyć m.in.:

- opracowanie w 2004 roku zestawu wskazówek dla bezpiecznych, międzynarodowych transakcji e-handlowych (*APEC Guidelines for Secure International E-Commerce Transactions*),
- organizację warsztatów poświęconych bezpieczeństwu sieci bezprzewodowych (w latach 2004—2006),
- opracowanie zestawu wskazówek i zasad mających podnieść stopień ochrony systemów SCADA w kontekście rosnącego zagrożenia cyberatakami wymierzonymi w infrastrukturę krytyczną (*E-Security Aspects of Essential Infrastructure Service*),
- przeprowadzenie wraz z Organizacją Współpracy Gospodarczej i Rozwoju (OECD) wspólnych warsztatów w Seulu (2005) dotyczących ochrony systemów i sieci informacyjnych (*APEC-OECD Workshop on Security of Information Systems and Networks*),
- organizację wraz z OECD w Manili w 2007 roku wspólnych warsztatów poświęconych zwalczaniu złośliwego oprogramowania (*APEC TEL — OECD Malware Workshop*),
- przygotowanie wraz z OECD wspólnego raportu na temat złośliwego oprogramowania i sposobów jego zwalczania (*APEC TEL — OECD Analytical Report on Malicious Software and Recommendations with Actions Plans against Malware and related Threat*),
- zorganizowanie wraz z ASEAN warsztatów w Manili w 2007 roku na temat bezpieczeństwa sieci (*APEC TEL and ASEAN Workshop on Network Security*),
- realizację projektów dotyczących sposobów uwierzytelniania w sieci (*APEC TEL PKI/E-Authentication Training Program*),
- rozpoczęcie programu dotyczącego walki z sieciami *botnet* (*Guide on Policy and Technical Approach against Botnet*),

[116] *Security and Prosperity Steering Group*. APEC: http://apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group.aspx; dostęp: 28.03.2014.

- organizację spotkań ekspertów ds. cyberbezpieczeństwa (*Cybercrime Experts Group Meetings*),
- organizację w 2011 roku warsztatów na temat rozwoju polityki cyberbezpieczeństwa w regionie Azji i Pacyfiku,
- wspieranie poszczególnych inicjatyw Organizacji Współpracy Gospodarczej i Rozwoju, w tym np. *OECD Principles for Internet Policy Making* czy *OECD Recommendation of the Council on the Protection of Children Online*,
- organizację wspomnianego już Dnia Świadomości Cyberbezpieczeństwa (*Cyber Security Awareness Day*)[117].

Co prawda na początku drugiej dekady XXI wieku intensywność prowadzonych przez APEC TEL prac nieco spadła, jednak i tak należy docenić ich pozytywne rezultaty. Mimo że *de facto* Współpraca Gospodarcza Azji i Pacyfiku miała przede wszystkim kompetencje w wymiarze gospodarczym w ciągu kilkunastu lat udało się jej wykształcić interesującą strategię walki z cyberzagrożeniami, która miała kilka cech charakterystycznych. Przede wszystkim, co naturalne, skupiła się ona niemal wyłącznie na cyberprzestępczości, pozostawiając inne wyzwania podmiotom bardziej do tego odpowiednim. Wypracowała ona wiele przydatnych dokumentów politycznych, które wskazywały na potrzebę pogłębiania kooperacji w tej dziedzinie, nie tylko między państwami, lecz także sektorem prywatnym i pozostałymi organizacjami międzynarodowymi. Prace koncepcyjne znalazły odzwierciedlenie w wielu wartościowych przedsięwzięciach w wymiarze praktycznym, które były realizowane przez Grupę Roboczą Telekomunikacji i Informacji. Przejawiały się ona głównie działaniami zmierzającymi do podnoszenia świadomości użytkowników na temat skali i charakteru zagrożeń pojawiających się w cyberprzestrzeni oraz sposobów ich zwalczania. APEC jako jedna z nielicznych struktur tego typu zawiązała bliską i skuteczną współpracę z innymi organizacjami międzynarodowymi. Za szczególnie owocne należy uznać przede wszystkim kontakty z Organizacją Współpracy Gospodarczej i Rozwoju.

[117] Za: *Security and Prosperity Steering Group*. APEC: http://apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group.aspx; dostęp: 28.03.2014; S.J. Shafie: *APEC TEL*, op.cit.; *2012 Cyber Security Awareness Day*. APEC: www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group/Cybersecurity-Awareness-2012.aspx; dostęp: 28.03.2014.

5.8. Inicjatywy Organizacji Współpracy Gospodarczej i Rozwoju w dziedzinie cyberbezpieczeństwa

Podobnie jak w przypadku APEC, Organizacja Współpracy Gospodarczej i Rozwoju (OECD) pozornie jest podmiotem, który nie powinien angażować się w działania na rzecz zwalczania zagrożeń teleinformatycznych, ponieważ głównym celem tej powstałej w 1960 roku struktury jest osiągnięcie jak najwyższego stopnia rozwoju gospodarczego, zatrudnienia i stabilności finansowej w państwach członkowskich (Bierzanek, Symonides, 2002: 332). W związku z coraz większą rolą odgrywaną w gospodarce światowej przez najnowsze technologie, w tym Internet, OECD była jednak niejako zmuszona zająć się bezpieczeństwem teleinformatycznym. Jak stwierdzono na stronie internetowej organizacji, głównym założeniem wysiłków na tym polu było zapewnienie, aby „gospodarka internetowa" nadal stanowiła platformę innowacji, a także źródło wzrostu ekonomicznego i społecznego[118].

OECD zainteresowała się problematyką zagrożeń komputerowych bardzo wcześnie, już bowiem w 1983 roku zdefiniowała ona cyberprzestępstwo jako „nielegalne, sprzeczne z etyką oraz nieautoryzowane działanie skutkujące automatyczną zmianą danych lub ich przesyłu". W 1985 roku opublikowano raport pod tytułem *Computer-related Criminality: Analysis of Legal Policy in the OECD Area*. W 1990 roku natomiast wyłoniono grupę specjalistów z zakresu matematyki, informatyki, prawa oraz biznesu, której celem były prace na rzecz ochrony prawnej systemów informacyjnych (Siwicki, 2013: 44—45; Bógdał-Brzezińska, Gawrycki, 2003: 222). Ich skutkiem było opublikowanie w 1992 roku pierwszego zestawu rekomendacji dla „bezpieczeństwa systemów informacyjnych" (*OECD Guidelines for the Security of Information Systems*). Był to wyjątkowy jak na ten okres, niewiążący dokument przyjęty przez organizację międzynarodową. Stwierdzono w nim, że w obliczu globalnych procesów proliferacji najnowszych technologii teleinformatycznych brakowało odpowiednich rozwiązań i zabezpieczeń. Zdaniem autorów pojawiały się nowe wyzwania, którym należało skutecznie przeciwdziałać. W zamyśle rekomendacje OECD miały więc m.in. rozwijać współpracę międzynarodową w tej dziedzinie, także między sektorem prywatnym i publicznym, podnosić świadomość zagrożeń komputerowych, jak również wspierać powstawanie nowych instrumentów i procedur ochrony systemów informacyjnych. Zaproponowano wówczas zestaw definicji kilku podstawowych pojęć, takich jak *dane*, *informacje*, *systemy informacyjne* czy *dostępność*, co miało ułatwić wdrażanie tego dokumentu w praktyce. Na tym tle wśród rekomendacji wymieniono m.in. poszanowanie praw i interesów

[118] *Information Security and Privacy*. Organisation for Economic Co-operation and Development: www.oecd.org/internet/ieconomy/informationsecurityandprivacy.htm; dostęp: 28.03.2014.

innych użytkowników, uwzględnienie wielowymiarowego podejścia do tych zagadnień, kompatybilność z wartościami demokratycznymi czy koordynację oraz integrację różnych procedur, instrumentów i mechanizmów ochrony systemów informacyjnych.

Założenia te miały być realizowane za pomocą odpowiednich rozwiązań politycznych i prawnych, szkoleń i edukacji, egzekwowania i dochodzenia roszczeń, wymiany informacji oraz współpracy na poziomie narodowym i ponadnarodowym[119]. Warto zauważyć, iż był to jeden z pierwszych wydanych przez organizację międzynarodową dokumentów, który w sposób tak dojrzały i zarazem tak wcześnie omówił podstawowe zagadnienia związane z bezpieczeństwem teleinformatycznym. Nie miał on wprawdzie żadnej mocy prawnej, wyznaczał jednak pewne standardy, które jak na początek lat 90. XX wieku były z pewnością nowatorskie. Nie przyczynił się on niestety do bardziej intensywnych prac w tej dziedzinie. W kolejnych latach OECD nawiązywała co prawda do tych problemów, jednak w sposób dość ograniczony. Można tu wymienić np. deklarację ministerialną na temat prywatności w sieci z grudnia 1998 roku czy rekomendację Rady OECD dotyczącą polityki kryptograficznej z marca 1997 roku (*Recommendation of the Council*, 1997; *Ministerial Declaration*, 1998).

Do pewnego przyspieszenia doszło dopiero w 2002 roku. Rada OECD opublikowała wówczas zestaw rekomendacji dotyczących bezpieczeństwa systemów informacyjnych oraz sieci zatytułowany *Towards a culture of security*, który aktualizował rozwiązania przyjęte w 1992 roku. Zauważając w nim rosnące uzależnienie gospodarek państw od prawidłowego funkcjonowania nowych technologii, sformułowano szereg propozycji skierowanych do państw członkowskich. Za główne cele dokumentu uznano:

- promocję kultury bezpieczeństwa jako środka ochrony systemów i sieci informacyjnych,
- podnoszenie świadomości na temat zagrożeń dla systemów i sieci informacyjnych,
- wspieranie większego zaufania wśród wszystkich użytkowników systemów i sieci informacyjnych,
- stworzenie ogólnych ram odniesienia, które wspomogłyby proces zrozumienia przez interesariuszy podstawowych problemów bezpieczeństwa,
- promocję współpracy oraz wymiany informacji między wszystkimi interesariuszami w procesie określania i implementacji polityk bezpieczeństwa,
- uznanie bezpieczeństwa za istotny cel przez wszystkich zaangażowanych interesariuszy.

[119] *OECD Guidelines for the Security of Information Systems*. Organisation for Economic Co-operation and Development, 1992: www.oecd.org/sti/ieconomy/oecdguidelinesforthesecuri tyofinformationsystems1992.htm; dostęp: 31.03.2014.

W punkcie II. wyznaczono podstawowe zasady, na których miała się oprzeć nowa kultura bezpieczeństwa teleinformatycznego: wskazano tu na potrzebę podnoszenia świadomości wszystkich zaangażowanych podmiotów, uznano odpowiedzialność wszystkich interesariuszy za cyberbezpieczeństwo, stwierdzono, że wszyscy uczestnicy powinni współdziałać w celu prewencji, wykrywania oraz reagowania na incydenty teleinformatyczne, zaakcentowano także potrzebę poszanowania interesów innych użytkowników, wskazano, że bezpieczeństwo sieci i systemów informacyjnych powinno być kompatybilne z wartościami demokratycznymi, a także zauważono, że uczestnicy powinni przeprowadzać badania możliwości wystąpienia incydentów teleinformatycznych, jak również uznać bezpieczeństwo za istotny element projektowania i tworzenia systemów i sieci informacyjnych. Stwierdzono, iż należy przyjąć kompleksowe, wielowymiarowe i dynamiczne podejście do reagowania kryzysowego, a na koniec podkreślono, iż uczestnicy powinni dokonać ponownej analizy zabezpieczeń sieci i systemów informacyjnych oraz dokonać odpowiednich modyfikacji (*Recommendation of the Council*, 2009: 81—83). Na tej podstawie w lipcu 2003 roku Dyrektoriat dla Nauki, Technologii i Przemysłu OECD (Directorate for Science, Technology and Industry) przyjął plan implementacji tego dokumentu. Określono w nim zadania, które powinny wypełniać rządy państw członkowskich, wśród których wymieniono m.in. opracowanie narodowych polityk cyberbezpieczeństwa, wspieranie innych interesariuszy, ocenę ryzyka oraz przestrzeganie podstawowych zasad etycznych. Wskazano na odpowiedzialność sektora prywatnego za bezpieczeństwo oferowanych produktów i usług wykorzystujących technologie informacyjne i komunikacyjne (*Implementation Plan*, 2003).

Te dwa dokumenty określające stosunek Organizacji Współpracy Gospodarczej i Rozwoju do cyberbezpieczeństwa na początku XXI wieku stanowiły podstawę kolejnych prac koncepcyjnych w kolejnych latach. W 2005 roku Dyrektoriat dla Nauki, Technologii i Przemysłu OECD przyjął raport, który określił stan wdrożenia założeń dokumentu z 2002 roku. Stwierdzono w nim pewne postępy, przede wszystkim jeśli chodzi o ochronę infrastruktury krytycznej, zwalczanie cyberprzestępczości oraz powstawanie zespołów CERT. Zauważono zarazem niewystarczającą ilość przedsięwzięć badawczo-rozwojowych (*The Promotion of a Culture*, 2005). W 2007 roku przyjęto z kolei raport poświęcony ochronie infrastruktury krytycznej (*Development of Policies*, 2007).

Ostatni ważny dokument Rada OECD przyjęła w 2008 roku. Został on poświęcony w całości ochronie infrastruktury krytycznej państw członkowskich. Odwołując się w nim do wcześniejszych osiągnięć oraz rezolucji Zgromadzenia Ogólnego ONZ nr 58/199, uchwalono wówczas kolejny zestaw rekomendacji. W części pierwszej wymieniono podstawowe zobowiązania państw członkowskich, w tym przyjęcie jasno określonych celów polityki ochrony infrastruktury krytycznej, wskazanie organów odpowiedzialnych za jej wdrożenie, przeprowa-

dzenie konsultacji z sektorem prywatnym, zapewnienie transparentności podziału obowiązków między poszczególnymi organami i strukturami, systematyczny przegląd polityk oraz regulacji prawnych, opracowanie narodowej strategii ochrony infrastruktury krytycznej, dokonywanie systematycznej oceny zagrożeń czy kooperację z sektorem prywatnym poprzez regularną wymianę informacji lub wspólne przedsięwzięcia badawczo-rozwojowe. W części drugiej wezwano natomiast państwa członkowskie do intensyfikacji współpracy ponadnarodowej, np. poprzez partycypację w międzynarodowych sieciach wczesnego ostrzegania przed zagrożeniami (*Recommendation of the Council*, 2009: 91—94). Dokument ten w zasadzie ograniczył się więc do powtórzenia pewnych podstawowych rozwiązań, które pojawiały się już wcześniej. Warto dodać, iż w grudniu 2013 roku OECD zdecydowała o rozpoczęciu prac nad jego aktualizacją[120].

Na tej podstawie Organizacja Współpracy Gospodarczej i Rozwoju zrealizowała szereg przedsięwzięć, których celem było stworzenie mechanizmów praktycznej współpracy na arenie międzynarodowej. Bezpośrednio za te działania odpowiedzialna była Grupa Robocza ds. Bezpieczeństwa Informacji oraz Prywatności (Working Party on Information Security and Privacy — WPISP). Do jej podstawowych kompetencji zaliczono prowadzenie analiz oraz formułowanie rekomendacji, które pomogłyby rządom oraz innym podmiotom zapewnić bezpieczeństwo teleinformatyczne oraz ochronę prywatności w sieci. O wielowymiarowym podejściu Grupy do tych problemów świadczył fakt, iż jej w skład wchodzili nie tylko eksperci z poszczególnych krajów członkowskich, ale także przedstawiciele sektora prywatnego czy środowiska naukowego. W założeniu WSISP pełni cztery rodzaje funkcji: postrzega bezpieczeństwo teleinformatyczne (informacyjne) oraz prywatność jako determinanty rozwoju „gospodarki internetowej", stanowi platformę pozwalającą decydentom polityki cyberbezpieczeństwa monitorować globalne trendy czy wymieniać się doświadczeniami, rozwija oraz nadzoruje wdrażanie kilku niewiążących porozumień w tej dziedzinie, stanowi rezerwuar ekspertów komputerowych. Grupa miała być zatem w założeniu organem wspierającym formułowanie narodowych polityk bezpieczeństwa teleinformatycznego, a także intensyfikującym międzynarodową współpracę w tej dziedzinie. W odróżnieniu jednak np. od Szanghajskiej Organizacji Współpracy OECD zdecydowało się utrzymywać ożywione stosunki zarówno z innymi organizacjami międzynarodowymi (APEC TEL, UE ENISA, Rada Europy), jak i z przedstawicielami sektora prywatnego (np. ITAC, CSISAC, BIAC)[121].

---

[120] *The OECD is revising its 2002 „Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"*. Organisation for Economic Co-operation and Development: www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm; dostęp: 31.03.2014.

[121] Business and Industry Advisory Committee to the OECD (BIAC), The Civil Society Information Society Advisory Council (CSISAC), The Internet Technical Advisory Committee

Warto wskazać na szereg najważniejszych przedsięwzięć Organizacji Współpracy Gospodarczej i Rozwoju w dziedzinie cyberbezpieczeństwa, które na większą skalę zaczęły być realizowane mniej więcej od połowy pierwszej dekady XXI wieku. Należy tu wymienić m.in.:

- organizację w październiku 2003 roku międzynarodowej konferencji poświęconej bezpieczeństwu systemów informacyjnych i sieci (*OECD Global Forum on Information Systems and Network Security: Towards a Global Culture of Security*)[122],
- organizację we wrześniu 2005 roku wspólnych z APEC warsztatów z zakresu bezpieczeństwa sieci i systemów informacyjnych; ich celem była wymiana opinii, doświadczeń i materiałów na temat polityk cyberbezpieczeństwa obu organizacji, a także wyodrębnienie przyszłych obszarów kooperacji (*APEC--OECD Workshop*, 2005),
- organizację w kwietniu 2007 roku wspólnych z APEC warsztatów poświęconych złośliwemu oprogramowaniu oraz sposobom jego zwalczania[123],
- opublikowanie w 2008 roku monografii i raportu poświęconych wpływowi złośliwego oprogramowania na rozwój „gospodarki internetowej" (zob. *Computer Viruses*, 2009; van Eeten, Bauer, 2008),
- opublikowanie w 2010 roku raportu na temat zwalczania sieci *botnet* (van Eeten, Bauer, Asghari, Tabatabaie, 2010),
- podjęcie badań nad politykami cyberbezpieczeństwa państw członkowskich od 2012 roku (zob. *Cybersecurity policy making*, 2012).

Oprócz wspomnianych wyżej inicjatyw OECD działała również na innych, pokrewnych obszarach, takich jak ochrona dzieci online, ochrona prywatności, ochrona praw autorskich, tożsamość elektroniczna czy kryptografia[124].

Reasumując ten wątek, należy podkreślić, iż dość nieoczekiwanie OECD stała się jedną z organizacji, które najwcześniej zwróciły uwagę na niekorzystne konsekwencje rewolucji informatycznej. Ze względu na pełnione funkcje skupiała się w swoich pracach przede wszystkim na kwestiach zwalczania przestępczości komputerowej, ochrony infrastruktury krytycznej oraz walki ze złośliwym oprogramowaniem, zagadnienia te postrzegano bowiem jako funda-

(ITAC). Zob. *What is the OECD Working Party on Information Security and Privacy (WPISP).* Organisation for Economic Co-operation and Development: www.oecd.org/sti/ieconomy/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm; dostęp: 31.03.2014.

[122] *OECD Global Forum on Information Systems and Network Security: Towards a Global Culture of Security.* Organisation for Economic Co-operation and Development, Oslo 13—14.10.2003: www.oecd.org/internet/ieconomy/8768646.pdf; dostęp: 31.03.2014.

[123] *APEC-OECD Malware Workshop.* Organisation for Economic Co-operation and Development, Manila 22—23.04.2007: www.oecd.org/internet/ieconomy/apec-oecdmalwareworkshop.htm; dostęp: 31.03.2014.

[124] *OECD instruments and reports on information security and privacy policy.* Organisation for Economic Co-operation and Development: www.oecd.org/sti/ieconomy/oecdinstrumentsandreportsoninformationsecurityandprivacypolicy.htm; dostęp: 31.03.2014.

mentalne dla stabilnego wzrostu gospodarczego, w tym głównie sektora IT. Państwa członkowskie nie były natomiast zainteresowane użyciem struktur organizacji do uregulowania problemów związanych z cyberatakami, które miały kontekst polityczny. Na tej podstawie, oceniając przedsięwzięcia OECD, można wysnuć trzy wnioski. Po pierwsze w wymiarze koncepcyjnym ograniczono się do formułowania pewnych podstawowych rekomendacji i zaleceń co do charakteru polityki cyberbezpieczeństwa. Choć wskazówki z 1992 roku należy uznać za nowatorskie, to późniejsze nie wykraczały raczej poza dość ogólne, sztampowe rozwiązania, przyjmowane przez inne organizacje międzynarodowe. Po drugie w wymiarze praktycznym skupiono się przede wszystkim na organizowaniu konferencji i warsztatów mających w zamyśle nie tylko podnosić zrozumienie specyfiki cyberzagrożeń, ale także ułatwiać międzynarodowy dialog w tej dziedzinie. Ponadto OECD przygotowała szereg interesujących prac badawczych, które dotyczyły głównie instrumentów wykorzystywanych przez przestępców komputerowych (*malware*, sieci *botnet*). Po trzecie unikalną cechą działań OECD była wspomniana już współpraca z APEC. Był to jeden z nielicznych przykładów wspólnych inicjatyw na tym polu podejmowanych przez dwie międzynarodowe organizacje gospodarcze.

5.9. Unia Afrykańska wobec zagrożeń dla bezpieczeństwa teleinformatycznego

Międzynarodowe przedsięwzięcia zmierzające do redukcji wyzwań pojawiających się w cyberprzestrzeni nie ograniczają się wyłącznie do obszaru Europy i Azji, są również widoczne na Czarnym Kontynencie, czego symbolem stała się Unia Afrykańska. Jako organizacja mająca bardzo rozległe funkcje, począwszy od obrony suwerenności i integralności terytorialnej państw członkowskich, przez rozwijanie współpracy międzynarodowej, aż po promocję ochrony praw człowieka (Bierzanek, Symonides, 2002: 334), UA stała się strukturą, która w naturalny sposób mogła odegrać istotną rolę w tej dziedzinie. Początkowo jednak kraje afrykańskie, starając się przeciwdziałać wyzwaniom dla bezpieczeństwa międzynarodowego, skupiały się głównie na zagrożeniach konwencjonalnych. Było to o tyle zrozumiałe, iż w odróżnieniu od wcześniej omówionych kontynentów w Afryce procesy komputeryzacji i informatyzacji w pierwszej dekadzie XXI wieku były mocno zapóźnione (Avila, 2009: 136—146).

Na tym tle pierwsze poważniejsze kroki zmierzające do wypracowania podstawowych mechanizmów kooperacji na Czarnym Kontynencie podjęły inne, komplementarne wobec UA organizacje. Chodziło tu przede wszystkim

o Wspólnotę Rozwoju Afryki Południowej (SADC), która w 2005 roku rozpoczęła działania na rzecz harmonizacji regulacji prawnych dotyczących zwalczania przestępczości komputerowej w państwach członkowskich[125]. W 2006 roku utworzyła ona Podkomitet Szefów Policji (Police Chiefs Sub-committee), którego funkcjonowanie obejmowało również zwalczanie cyberprzestępczości[126]. Nieco później pierwsze wysiłki na polu bezpieczeństwa teleinformatycznego podjęły również kraje Afryki Wschodniej, choć tam przebiegały one zdecydowanie wolniej[127]. Wyrazem regionalnego zainteresowania tą tematyką była organizacja szczytu *Connect Africa* w październiku 2007 roku, nad którym patronat objęła Rwanda. Wzięło w nim udział w sumie ok. 1000 uczestników, przede wszystkim z państw afrykańskich. Jego podstawowym założeniem był wprawdzie rozwój afrykańskiego sektora ICT, wśród celów konferencji wymieniono jednak również „przyjęcie narodowych e-strategii, w tym ram cyberbezpieczeństwa"[128]. Wszystkie powyższe inicjatywy podejmowały co prawda wątek bezpieczeństwa teleinformatycznego, czyniły to jednak w sposób bardzo ograniczony, nie doprowadziły one zatem do wykształcenia jakichkolwiek wartościowych mechanizmów kooperacji w Afryce. Za wyraźny sygnał znaczących zapóźnień można uznać fakt, iż do 2013 roku jedynie 11 państw afrykańskich utworzyło zespoły reagowania na incydenty komputerowe (CERT)[129].

Na początku drugiej dekady XXI wieku bezpieczeństwem teleinformatycznym zainteresowała się w końcu Unia Afrykańska, jej aktywność w tej dziedzinie okazała się jednak dość jednowymiarowa, ponieważ cały wysiłek skupiono na opracowaniu projektu pierwszej wspólnej dla całego kontynentu konwencji w sprawie ustanowienia ram prawnych dla cyberbezpieczeństwa (*Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa*). Warto szerzej scharakteryzować zapisy tego dokumentu, który został oparty na kilku strategicznych założeniach, takich jak ustanowienie zasad współpracy w kluczowych obszarach cyberbezpieczeństwa UA, regulacja elektronicznych reklam, transakcji oraz podpisów czy określenie podstawowych norm prawnych dotyczących zwalczania cyberprzestępczości. W jego części pierwszej omówiono najważniejsze sprawy związane z handlem elektronicznym i zaproponowano podstawowe definicje takich terminów, jak *szyfrowanie* czy *poczta elektroniczna*. Scharakteryzowano ponadto obowiązki państw,

[125] *Global Strategic Report*. International Telecommunication Union: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapt_1_iframe.htm; dostęp: 2.04.2014.

[126] *Police (SARPCCO)*. Southern African Development Community: www.sadc.int/themes/politics-defence-security/police-sarpcco; dostęp: 2.04.2014.

[127] *Global Strategic Report*. International Telecommunication Union: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapt_1_iframe.htm; dostęp: 2.04.2014.

[128] *Connect Africa Summit. Outcomes Report*. Connect Africa Summit, 5.12.2007, s. 2.

[129] R. Wanjiku: *Africa increases cybersecurity efforts*. IT World, 21.06.2013: www.itworld.com/security/362093/africa-increases-cybersecurity-efforts; dostęp: 2.04.2014.

kwestię reklam elektronicznych, a także umów i transakcji zawieranych online. Część drugą poświęcono ochronie danych osobowych. Również tutaj rozpoczęto od krótkiego omówienia najważniejszych terminów, takich jak *wrażliwe dane* czy *przetwarzanie danych*. Dalej natomiast zobowiązano kraje członkowskie do ustanowienia ram prawnych, które pozwoliłyby skutecznie zwalczać naruszenia prawa do prywatności w Internecie, a także do utworzenia organów uprawnionych do ochrony danych osobowych w cyberprzestrzeni. Najważniejsza część trzecia skupiła się na promocji cyberbezpieczeństwa oraz zwalczaniu przestępczości komputerowej. W sekcji pierwszej omówiono więc podstawowe pojęcia, takie jak *komunikacja elektroniczna*, *dane komputerowe*, *system komputerowy* czy *uszkodzenia*. Na tej podstawie w kolejnych artykułach zobowiązano państwa członkowskie m.in. do opracowania narodowych polityk cyberbezpieczeństwa, przyjęcia skutecznych środków prawnych zwalczania przestępczości komputerowej, do utworzenia organów odpowiedzialnych za te działania, zapewnienia, iż przyjęte rozwiązania nie będą godziły w prawa człowieka, ochrony infrastruktury krytycznej, rozwoju kultury cyberbezpieczeństwa, rozwoju partnerstwa publiczno-prywatnego, podjęcia działań edukacyjnych i szkoleniowych, harmonizacji rozwiązań prawnych i penalizacji cyberataków (*Draft African Union Convention*, 2012).

Treść projektu konwencji Unii Afrykańskiej można oceniać z dwóch perspektyw. Z jednej strony jej zapisy w znacznym stopniu różniły się od dokumentów i regulacji przyjmowanych przez inne organizacje regionalne, takie jak chociażby Rada Europy. Przejawem tego było nie tylko uwzględnienie takich zagadnień, jak ochrona danych osobowych czy e-handel, ale także bardzo ogólnikowe potraktowanie samej problematyki zagrożeń teleinformatycznych. Co prawda zestaw działań, które miały podjąć poszczególne rządy, należy uznać za właściwy, zabrakło tutaj jednak bardziej szczegółowej charakterystyki tych obowiązków. Mimo to część badaczy, w tym np. Tim Akano, uznało konwencję za „dobry krok we właściwym kierunku”[130]. Z drugiej jednak strony należy podkreślić, iż projekt traktatu wywołał poważne kontrowersje, przede wszystkim wśród przedstawicieli sektora prywatnego oraz szeroko pojętego środowiska naukowego. Zarzucali oni autorom pominięcie ich sugestii, a także niedostateczne zaakcentowanie wagi ochrony praw człowieka, ponieważ część zapisów była sformułowana na tyle ogólnikowo, że mogła posłużyć reżimom autorytarnym do łamania prawa do prywatności motywowanego podejrzeniem zagrożeniem dla bezpieczeństwa państwa[131]. Związane z tym wątpliwości oka-

[130] J. Silberberg: *African Union set to get tougher on cybercrime*. SciDev.net, 30.12.2013: www.scidev.net/global/digital-divide/news/african-union-set-to-get-tougher-on-cybercrime.html; dostęp: 2.04.2014.

[131] J. Macharia: *Africa Needs A Cybersecurity Law but AU's Proposal is Flawed, Advocates Say*. TechPresident, 31.01.2014: http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed; dostęp: 2.04.2014.

zały się na tyle duże, iż Unia Afrykańska w styczniu 2014 roku zdecydowała o odłożeniu w czasie przyjęcia konwencji[132]. Warto jednak zauważyć, iż mimo fiaska w tej sprawie na Czarnym Kontynencie równolegle były podejmowane inne przedsięwzięcia, których celem było zbudowanie mechanizmów regionalnej współpracy w dziedzinie cyberbezpieczeństwa, o czym świadczyły takie inicjatywy, jak np. *Africa Internet Summit,* który został zorganizowany w czerwcu 2013 roku[133].

Reasumując, warto zauważyć, iż na początku XXI wieku problem zagrożeń teleinformatycznych został, ze zrozumiałym opóźnieniem, zauważony także na kontynencie afrykańskim. Niestety ze względu na wczesne stadium tamtejszej rewolucji informatycznej działania poszczególnych państw i organizacji międzynarodowych były stosunkowo ubogie w treści. Jedynym w zasadzie wyjątkiem od tych niekorzystnych tendencji stała się konwencja Unii Afrykańskiej, która bardzo szeroko ujęła zagadnienia związane z cyberbezpieczeństwem. Mimo szeregu wartościowych zapisów spotkała się ona jednak z wieloma uzasadnionymi zarzutami, które w konsekwencji doprowadziły do zablokowania tego przedsięwzięcia. Dowodziło to, że zrozumienie specyfiki zagrożeń teleinformatycznych na Czarnym Kontynencie było nadal niewielkie. Powolne tempo prac nad przyjęciem tego dokumentu świadczyło zarazem o braku zainteresowania tamtejszych elit politycznych przeciwdziałaniem wyzwaniom pojawiającym się w cyberprzestrzeni. Można więc stwierdzić, że na początku XXI wieku w Afryce nie udało się wykształcić niezbędnych mechanizmów zwalczania takich zjawisk, jak cyberprzestępczość czy cyberterroryzm. Było to o tyle istotne, iż ze względu na globalny charakter Internetu mogło wpływać na bezpieczeństwo państw położonych również w innych częściach świata.

---

[132] M. Atagana: *15 key trends shaping Kenya's social and digital media landscape.* Yahoo! News, 20.03.2014: https://za.news.yahoo.com/15-key-trends-shaping-kenya-social-digital-media-111728767.html; dostęp: 2.04.2014.

[133] R. Wanjiku: *Africa increases cybersecurity efforts*..., op.cit.

Zakończenie

Rewolucja informatyczna, która rozpoczęła się na dobre w drugiej połowie XX wieku, w ciągu zaledwie kilku dekad w zasadniczym stopniu zmieniła oblicze świata w niemal wszystkich możliwych wymiarach i płaszczyznach. Zgodnie z przewidywaniami części deterministów technologicznych procesy komputeryzacji i informatyzacji objęły szybko kolejne dziedziny życia jednostek i ich zbiorowości, począwszy od gospodarki, przez naukę, rozrywkę, aż po politykę i wojskowość. Ze względu na jej najbardziej doniosłe cechy polegające na przezwyciężeniu dotychczasowych ograniczeń związanych z przetwarzaniem, przesyłaniem i przechowywaniem informacji przyniosła ona ludzkości ogromne korzyści. Ich symbolem stało się powstanie nowej, unikalnej w swojej istocie domeny, jaką jest cyberprzestrzeń. Jej specyficzne cechy sprawiają, że od dekad w coraz większym stopniu determinuje ona funkcjonowanie państw i społeczeństw, przenikając administrację państwową, infrastrukturę krytyczną, sektor biznesowy czy siły zbrojne. Ich rosnące uzależnienie od ICT stało się jednak zarazem powodem pojawiania się pewnych negatywnych tendencji, których koszty ponoszone są na całym świecie. Powszechność i globalny charakter technologii teleinformatycznych doprowadziły do epokowych zmian w szeroko pojętym środowisku bezpieczeństwa, ponieważ komputery i ich sieci, przyczyniając się do rewolucji w sprawach wojskowych (RMA), stały się równolegle źródłem i platformą szkodliwych zjawisk, które z czasem zaczęły być postrzegane przez pryzmat zagrożeń dla bezpieczeństwa narodowego i międzynarodowego. Rozmaite podmioty, począwszy od zwykłych amatorów, hakerów, przez haktywistów, cyberterrorystów, na organizacjach przestępczych skończywszy, dzięki cyberprzestrzeni zyskały możliwość dotarcia nawet do najbardziej żywotnych elementów systemów bezpieczeństwa państw. Innymi słowy cyberprzestrzeń paradoksalnie stała się kolejnym wymiarem bezpieczeństwa, którego rola

rośnie proporcjonalnie do postępów procesów komputeryzacji i informatyzacji. Jeszcze w latach 90. XX wieku nawet najpoważniejsze ataki komputerowe były z reguły uznawane co najwyżej za pewną niedogodność dla administracji centralnej, tymczasem już dwie dekady później ich skala stała się na tyle duża, iż zaczęto upatrywać w nich jednego z najpoważniejszych wyzwań dla stabilności całego systemu międzynarodowego.

W tym nowym środowisku, jakim jest cyberprzestrzeń, unikalnym podmiotem pozostają państwa, które jeszcze do niedawna nie wykazywały zwiększonego zainteresowania rozwijaniem własnych zdolności do działania w tej sferze. Zaczęło się to zmieniać mniej więcej na przełomie XX i XXI wieku, kiedy wynikające z tego potencjalne korzyści dostrzegły elity polityczne zaledwie kilku krajów, takich jak Stany Zjednoczone, Rosja, Chiny czy Izrael. Z jednej strony zainicjowano prace nad rozbudową potencjału eksperckiego i technologicznego, który pozwalał efektywniej bronić się przed włamaniami do sieci komputerowych. Z drugiej zrozumiano, że ofensywna aktywność w przestrzeni teleinformatycznej może stać się dogodnym orężem rywalizacji i konfrontacji z innymi podmiotami w środowisku międzynarodowym. Sprzyjały temu obiektywne właściwości tej domeny, takie jak łatwa do osiągnięcia anonimowość, „ageograficzność" i „aterytorialność" czy niskie koszty „wejścia". Ponadto na przydatność tych instrumentów wskazywały niejasności związane z interpretacją obowiązujących zapisów prawa międzynarodowego oraz mechanizmów współpracy politycznej i wojskowej. Prekursorzy ci w ciągu zaledwie kilku lat wykształcili więc zaawansowane zdolności w tym zakresie, które mogły w teorii posłużyć do realizacji określonych celów na wybranych kierunkach.

Przeanalizowane w pracy przypadki rywalizacji i współpracy państw w cyberprzestrzeni dają podstawę do potwierdzenia postawionych we wstępie hipotez. Zgodnie z hipotezą główną przestrzeń teleinformatyczna rzeczywiście stała się nowym wymiarem polityki zagranicznej, ponieważ rządy w XXI wieku coraz częściej wykorzystują cyberataki, aby realizować swoje interesy w środowisku międzynarodowym, co implikuje zjawisko ich rywalizacji. Ze względu na jej właściwości środki te jawią się jako dogodna, choć posiadająca zróżnicowaną skuteczność metoda osiągania celów na arenie międzynarodowej, o czym świadczyło dobitnie wiele scharakteryzowanych w poprzednich rozdziałach wydarzeń. Przede wszystkim jednym z pierwszych państw, które zdecydowało się na wykorzystanie w ten sposób cyberprzestrzeni, była Chińska Republika Ludowa, która na początku XXI wieku zdecydowała się wpleść ofensywne operacje w tej sferze w całokształt narastającej rywalizacji strategicznej ze Stanami Zjednoczonymi. Jej aktywność online przejawiała się wieloma incydentami, które miały charakter głównie cyberszpiegowski. Początkowo stały za nimi grupy chińskich haktywistów patriotycznych podejmujących akcje w momentach szczególnego napięcia w relacjach bilateralnych. Z czasem Pekin zdecydował o zaangażowaniu swoich sił zbrojnych, co wykazał m.in. przytoczony raport Mandiant. Odtąd roz-

poczęły się wielomiesięczne kampanie polegające na włamywaniu się do sieci komputerowych należących zarówno do sektora publicznego, jak i prywatnego USA, których celem było zdobycie jak największej ilości wrażliwych informacji dotyczących amerykańskich zasobów wojskowych, rozwiązań organizacyjnych i prawnych, planów i strategii czy wreszcie najnowszych technologii, zarówno cywilnych, jak i militarnych. Oczywistym zamysłem chińskich decydentów było więc zasypanie przepaści w potencjałach miedzy ChRL a USA. Ostatnie osiągnięcia chińskich naukowców zdają się potwierdzać, że cel ten przynajmniej częściowo osiągnięto[1]. Było to o tyle ważne, iż poprawiało pozycję Pekinu w coraz bardziej intensywnej rozgrywce z Waszyngtonem, upatrującym w nim swojego głównego przeciwnika w XXI wieku. Za równie istotne należy uznać także wykradanie wrażliwych danych dotyczących funkcjonowania amerykańskiej infrastruktury krytycznej oraz planów wojskowych, co można interpretować jako próbę przygotowania się do ewentualnego konfliktu zbrojnego na Pacyfiku, a więc także jako element odstraszania USA w Azji Wschodniej. Co ciekawe, jak okazało się w ostatnich latach, również Stany Zjednoczone prowadziły operacje w cyberprzestrzeni wymierzone w ChRL, których założeniem było m.in. osłabienie legitymizacji władz tego kraju czy ograniczenie jego zdolności do działania w tej domenie. Natężenie cyberataków z obu stron stało się na tyle duże, iż osiągnęło skalę cyberwojny. Wpłynęła ona zresztą w znacznym stopniu na oficjalny wymiar relacji bilateralnych. Nie przypadkiem zagadnienie to stało się jednym z głównych punktów rozmów w trakcie szczytu chińsko-amerykańskiego w czerwcu 2013 roku[2]. Na tej podstawie można więc stwierdzić, iż cyberprzestrzeń, stając się areną rywalizacji obu krajów, pozwoliła realizować trzy grupy celów polityki zagranicznej: bezpieczeństwo (dzięki zdobyciu technologii czy planów wojskowych), wzrost siły i potęgi (dzięki wykorzystaniu zdobytych osiągnięć naukowo-technicznych w praktyce), pozycja na arenie międzynarodowej (przyczyniając się do relatywnego osłabienia pozycji USA).

Instrumentalnie cyberataki traktowała także Federacja Rosyjska, która dostrzegała ich przydatność głównie na obszarze poradzieckim. Realizując podstawowe cele polityki zagranicznej w tym regionie, takie jak odzyskanie wpływów politycznych, ochrona mniejszości rosyjskiej czy podkopywanie międzynarodowej pozycji państw bałtyckich, działała równolegle na wielu płaszczyznach. Pod koniec pierwszej dekady XXI wieku jedną z nich stała się cyberprzestrzeń, którą wykorzystywano w dwojaki sposób. Z jednej strony użyteczne stały się kontakty z grupami cyberprzestępczymi (RBN). Najbardziej ewidentnym przy-

[1] Zob. B. Gertz: *Top Gun takeover: Stolen F-35 secrets showing up in China's stealth fighter*. „The Washington Times" 13.03.2014: www.washingtontimes.com/news/2014/mar/13/f-35-secrets-now-showing-chinas-stealth-fighter/?page=all; dostęp: 19.05.2014.

[2] D. Roberts: *US — China summit ends with accord on all but cyber-espionage*. „The Guardian" 10.06.2013: www.theguardian.com/world/2013/jun/09/us-china-summit-barack-obama-xi-jinping; dostęp: 16.05.2014.

kładem tego stanu rzeczy była wojna z Gruzją w sierpniu 2008 roku. Był to szczególny przypadek, ataki komputerowe zostały bowiem wówczas ściśle skoordynowane z konwencjonalnymi operacjami zbrojnymi. Co prawda nie doprowadziły one do naruszenia elementów gruzińskiej infrastruktury krytycznej, ale w znaczącym stopniu utrudniły politykę informacyjną Tbilisi, a co za tym idzie: ułatwiły propagandę wojenną Kremla, Gruzja utraciła bowiem w znacznej mierze możliwość prezentowania swojego stanowiska za pomocą Internetu. Działania w przestrzeni teleinformatycznej były więc jednym z czynników, które osłabiły pozycję Gruzji na arenie międzynarodowej, a więc współgrały z rosyjską racją stanu. Z drugiej strony odmienną specyfikę miały wydarzenia w Estonii i na Litwie, gdzie główną rolę odegrali haktywiści patriotyczni. W pierwszym przypadku stosującym dość proste metody sprawcom udało się nie tylko zablokować kluczowe strony internetowe, lecz także w pewnym sensie zaszkodzić elementom infrastruktury krytycznej (system finansowy). Tym samym ukarano Tallin za wrogą Federacji politykę historyczną oraz stosunek do mniejszości rosyjskiej. Zdołano także symbolicznie zaszkodzić wizerunkowi Estonii jako modelowemu przykładowi transformacji ustrojowej. Tymczasem na Litwie incydenty miały mniej poważny charakter, lecz również wpisywały się w logikę polityki Kremla wobec tego kraju. W obu przypadkach haktywiści patriotyczni starali się wspierać rosyjską rację stanu, udział władz FR miał tu więc raczej charakter pośredni, wynikający z zachęcania lub tolerowania tego typu bezprawnych zachowań na swoim terytorium. Co za tym idzie, cyberataki takie stały się w pewnym sensie *quasi*-instrumentem polityki zagranicznej, stosowanym samoistnie lub na wyraźny sygnał w momentach kryzysu w stosunkach z krajami obszaru poradzieckiego. Pomijając niejasny *casus* Kirgistanu, można więc zauważyć, iż Rosja wykorzystywała cyberprzestrzeń jako nowy wymiar oddziaływań w tym regionie, przydatny do realizacji trzech grup celów: wzrostu siły państwa, wzrostu jego pozycji międzynarodowej oraz zapewnienia bezpieczeństwa. Specyficzną cechą jej aktywności było użycie grup haktywistycznych i cyberprzestępczych, co pozwalało odciąć się od odpowiedzialności za organizację tych operacji. Pewnym potwierdzeniem tego stanu rzeczy były incydenty teleinformatyczne, które wystąpiły podczas kryzysu na linii Rosja — Ukraina w 2014 roku. Co prawda ani jedna, ani druga strona nie zdecydowała się na przeprowadzenie poważnych cyberataków, jednak ataki mniej groźne organizowali niezależnie haktywiści patriotyczni[3].

Następnym przykładem użyteczności ataków komputerowych do realizacji celów polityki zagranicznej były działania podejmowane przez Izrael przy wsparciu USA. Prawdopodobnie po raz pierwszy wykorzystał je w ten sposób

[3] J. Hsu: *Why There's No Real Cyberwar in the Ukraine Conflict*. „IEEE Spectrum" 14.03.2014: http://spectrum.ieee.org/tech-talk/computing/networks/why-theres-no-real-cyberwar-in-the-ukraine-conflict; dostęp: 17.05.2014.

we wrześniu 2007 roku, kiedy umiejętnie połączono akcję w cyberprzestrzeni z konwencjonalną operacją zbrojną o kryptonimie *Orchard*. Paraliżując system obrony przeciwlotniczej Syrii, pozwoliła ona na zbombardowanie budowanego reaktora atomowego, a tym samym na usunięcie żywotnego zagrożenia dla bezpieczeństwa narodowego. Na zdecydowanie wyższą ocenę zasługują jednak cyberataki wymierzone w Iran. Stworzenie szeregu zaawansowanych złośliwych programów z rodziny *Stuxnet* (*Duqu*, *Flame*) dowiodło, że głosy wskazujące na rychłe pojawienie się pierwszych cyberbroni nie były bezzasadne. Wykorzystanie przez Tel Awiw i Waszyngton robaka komputerowego przeciwko programowi atomowemu reżimu ajatollahów pozwoliło w niekonwencjonalny sposób spowolnić proces wzbogacania uranu, odsunięto zatem w czasie widmo powstania szyickiej broni jądrowej, która stanowiłaby zagrożenie dla obu państw. Jeszcze bardziej zaawansowane były akcje cyberszpiegowskie, które — choć nie zaszkodziły bezpośrednio infrastrukturze krytycznej Teheranu — pozwoliły zapewne zebrać wrażliwe informacje na jej temat. Jeśli natomiast ich celem było wywarcie dodatkowego nacisku na reżim, to w perspektywie krótkoterminowej nie udało się tego osiągnąć. Warto zauważyć, że i w tym wypadku można było dostrzec rywalizację w cyberprzestrzeni, która czasami przekształcała się wręcz w konfrontację. Odpowiadając na cyberataki Izraela i USA, Iran stosunkowo szybko sam zaczął przeprowadzać tego typu operacje, choć ich skuteczność była zdecydowanie niższa.

Można także wskazać na specyficzny *casus* Korei Północnej. Phenian od lat słynie z polityki zagranicznej, która w dużej mierze polega na naprzemiennym stosowaniu prowokacji oraz prób rekoncyliacji. Stosuje do tego rozmaite instrumenty, zarówno o charakterze politycznym, propagandowym, jak i *stricte* wojskowym. W tym kontekście dość szybko dostrzeżono, że cyberataki mogą być kolejną metodą pośredniego oddziaływania na środowisko międzynarodowe, w tym głównie na Koreę Południową oraz Stany Zjednoczone. Było to tym bardziej ewidentne, iż sama KRLD ze względu na ogromne zapóźnienia technologiczne była *de facto* odporna na ewentualne próby odpowiedzi w cyberprzestrzeni. W związku z tym od końca pierwszej dekady XXI wieku reżim zaczął organizować operacje cyberterrorystyczne i cyberszpiegowskie, którym przyświecały dwie grupy celów. Z jednej strony miały one stanowić kolejny element nacisku na Seul oraz Waszyngton, aby podejmowały decyzje zgodne z interesem Korei Północnej. Stosowano je równolegle z prowokacjami na innych polach, w tym m.in. próbnymi wybuchami jądrowymi, testami rakiet balistycznych, agresywnymi deklaracjami politycznymi czy incydentami zbrojnymi. Z drugiej strony celem kampanii wywiadowczych było uzyskanie wrażliwych informacji dotyczących systemu obronnego bądź infrastruktury krytycznej Korei Południowej, co mogłoby zostać wykorzystane w trakcie ewentualnego konfliktu na Półwyspie. Początkowo kampanie te miały dość prosty charakter, jednak z czasem poziom ich zaawansowania zaczął rosnąć. Mimo to efektywność cyberata-

ków była raczej znikoma, Phenianowi nie udało się bowiem wymusić na władzach Korei Południowej oraz Stanów Zjednoczonych korzystnych dla siebie decyzji.

Wszystkie powyższe przykłady zdają się potwierdzać słowa Jose Nazario (2009), który pisał:

> niska cena oraz duża dostępność instrumentów i broni — armii *botnet*, grup hakerów i tym podobnych — sprawiły, iż rządy z całego świata spoglądają na takie podejście jako metodę uciszania wrogów. Nawet jeśli nie ma bezpośredniego powiązania z rządem, takie akcje mogą działać na korzyść rządzącej partii.

Cyberataki przeprowadzane przez wojsko, agencje rządowe lub powiązane z nimi grupy stają się współcześnie coraz częstszym środkiem realizacji rozmaitych celów (politycznych, wojskowych, gospodarczych, ideologicznych) na arenie międzynarodowej. Mogą mieć one charakter cyberterrorystyczny, cyberszpiegowski, a także militarny, związany z realizacją określonej operacji zbrojnej. Oprócz nich unikalną rolę odgrywają grupy haktywistów patriotycznych, które korzystając z przyzwolenia niektórych państw, wspierają ich interesy w środowisku teleinformatycznym. Skuteczność tych instrumentów bywa jednak różna. W specyficznych warunkach potrafią one z powodzeniem zastąpić tradycyjne metody polityki zagranicznej: wyrazem tego była historia robaka *Stuxnet*. W innych ich efektywność bywa znikoma, o czym wielokrotnie przekonały się władze Korei Północnej. Na tym tle można pokusić się o stwierdzenie, iż z reguły cyberataki mają charakter komplementarny w stosunku do innych środków polityki zagranicznej. Stało się to widoczne np. w strategii Federacji Rosyjskiej na Kaukazie, gdzie incydenty teleinformatyczne wpisały się w konwencjonalny konflikt zbrojny, pozwalając Moskwie pełniej zrealizować wyznaczone priorytety. Podobnie było z chińskim cyberszpiegostwem, które uzupełniało, lecz nie zastępowało tradycyjnej aktywności wywiadowczej[4]. Co za tym idzie, można potwierdzić zjawisko rywalizacji, a czasami wręcz konfrontacji wybranych krajów w przestrzeni teleinformatycznej, występowały tam bowiem dwa niezbędne do tego elementy: sprzeczność interesów oraz uznanie danego podmiotu za rywala. Było to szczególnie ewidentne w przypadku relacji amerykańsko-chińskich, izraelsko-irańskich oraz międzykoreańskich.

Przeniesienie naturalnego procesu ścierania się interesów państw w środowisko cyberprzestrzenne ma poważne konsekwencje dla całej społeczności międzynarodowej. Przede wszystkim rywalizacja w tym wymiarze przyczyniła się do znacznego podniesienia skali zagrożeń teleinformatycznych. Obok haktywi-

[4] Zob. Y. Bhattacharjee: *How the F.B.I Cracked a Chinese Spy Ring*. „The New Yorker" 16.05.2014: www.newyorker.com/online/blogs/newsdesk/2014/05/how-the-fbi-cracked-a-chinese-spy-ring.html; dostęp: 19.05.2014.

zmu, cyberterroryzmu czy cyberprzestępczości, pojawiło się np. zjawisko cyberwojny. Jako że państwa — oprócz niektórych korporacji transnarodowych — dysponują największym potencjałem w tej dziedzinie, ich ofensywna aktywność może przyczyniać się do powstawania poważnych szkód, zarówno w wymiarze materialnym, jak i niematerialnym. Po drugie powstało pytanie, w jaki sposób należy interpretować obowiązujące dotychczas normy prawa międzynarodowego publicznego, w tym przede wszystkim te, które wynikają z *Karty Narodów Zjednoczonych*. Kwestia ta ma fundamentalne znaczenie, ponieważ może osłabiać ich skuteczność w nowym środowisku bezpieczeństwa XXI wieku. Po trzecie pod znakiem zapytania stanęło wiele mechanizmów międzynarodowej współpracy politycznej i wojskowej, ponieważ zapisy umów zawartych w okresie zimnej wojny nie są z reguły dostosowane do dylematów związanych z reagowaniem na cyberataki. Dowodem potwierdzającym ten stan rzeczy była omówiona bezradność NATO wobec incydentów teleinformatycznych w Estonii.

Przeciwdziałanie tym problemom na poziomie państwowym jest oczywiście niemożliwe, posiadająca globalny zasięg cyberprzestrzeń wymaga bowiem globalnych rozwiązań. W związku z tym zasadnicze znaczenie zyskała współpraca międzynarodowa w tym wymiarze. Jak słusznie stwierdził Kenneth Geers (2011: 123), „świat stał się tak uzależniony od Internetu, że rządy mogą szukać daleko idących, strategicznych rozwiązań, aby zapewnić sobie bezpieczeństwo […]. W konsekwencji […] bezpieczeństwo sieciowe nie jest już luksusem, lecz koniecznością". Pierwsze kroki zmierzające do nawiązania kooperacji w tej dziedzinie poczyniono stosunkowo wcześnie, już w latach 80. i 90. XX wieku. Choć miały one bardzo zróżnicowany charakter, to ich podstawowym celem była optymalizacja reguł funkcjonowania środowiska międzynarodowego w taki sposób, aby skutecznie przystosować je do pojawienia się cyberprzestrzeni. Według Kathariny Ziolkowski (2013: 13) ostatecznym celem było wzmocnienie światowego pokoju i bezpieczeństwa, eliminacja powodów wzajemnej nieufności, strachu czy niezrozumienia, a także prewencja konfrontacji zbrojnych. Oczywiście potencjalnie największą rolę w tym zakresie mogła odegrać Organizacja Narodów Zjednoczonych. Jak stwierdzono w ostatnim rozdziale, chociaż organy główne ONZ stosunkowo wcześnie zainteresowały się tą problematyką, to skuteczność ich zabiegów znacząco się rozmijała z oczekiwaniami i nawet najbardziej podstawowymi potrzebami. Co prawda ONZ wypracowała szereg interesujących dokumentów poświęconych tworzeniu globalnej kultury bezpieczeństwa czy walce z cyberprzestępczością, nie przekładało się to jednak z reguły na bezpośrednie, praktyczne przejawy współpracy państw. Najbardziej ewidentnym dowodem słabości Organizacji Narodów Zjednoczonych była bezczynność Rady Bezpieczeństwa, która ani razu nie podjęła starań zmierzających do uregulowania podstawowych zagadnień związanych z cyberbezpieczeństwem. Bezwładność ONZ wynikała głównie z głębokiego podziału, który ujawnił się w łonie społeczności międzynarodowej, na dwa obozy posiadające

diametralnie różne priorytety w tej dziedzinie. W zasadzie jedynym wyjątkiem od tej reguły był Międzynarodowy Związek Telekomunikacyjny. Była to jedyna organizacja o zasięgu globalnym, która w ciągu raptem kilku lat wypracowała wielowymiarowe i — co najważniejsze — skuteczne mechanizmy przeciwdziałania znacznej części zagrożeń bezpieczeństwa teleinformatycznego. Szczególnie wartościowe okazało się funkcjonowanie ITU-IMPACT. Niemniej można zauważyć, iż aktywność tej organizacji skupiała się przede wszystkim na praktycznym zwalczaniu wyzwań pojawiających się w cyberprzestrzeni. Tymczasem wszelkie próby uregulowania bardziej kontrowersyjnych kwestii, takich jak koncepcja „cyberpokoju", stale napotykały opór, głównie ze strony państw rozwiniętych. Tym samym także w ramach ITU ujawnił się rozłam na zwolenników i przeciwników zawarcia globalnego traktatu poświęconego rywalizacji i konfrontacji rządów w sieci, który paraliżował wszystkie bardziej ambitne inicjatywy. „Zimna wojna" w tej dziedzinie między USA i krajami zachodnimi z jednej strony a Rosją i Chinami z drugiej wynikała przede wszystkim z faktu, iż obie te grupy przyjęcie określonego modelu współpracy międzynarodowej postrzegały przez pryzmat interesów narodowych, a nie interesów całej społeczności międzynarodowej. Ta patowa sytuacja była więc bardzo niekorzystna i osłabiała skuteczność prawa międzynarodowego, na co zresztą wskazywała m.in. ChRL.

Osobna grupa inicjatyw dotyczących cyberbezpieczeństwa była podejmowana na szczeblu regionalnym przez wiele organizacji międzynarodowych. Najbardziej zaawansowane prace w tej dziedzinie prowadzone były w XXI wieku przez państwa zachodnie. Z jednej strony można zwrócić uwagę na Pakt Północnoatlantycki, który jako jedyny sojusz wojskowy na świecie wykształcił tak zaawansowaną strategię zwalczania cyberzagrożeń, opartą na systemie wzajemnie wspierających się instytucji. Szczególnie wartościową rolę odgrywa tu działające w Tallinie Centrum Doskonalenia Cyberobrony. Na uznanie zasługuje również decyzja z czerwca 2014 roku o zaliczeniu bezpieczeństwa teleinformatycznego do kolektywnej obrony NATO, co od wielu lat postulowali m.in. politycy estońscy. Niestety, mimo tego przełomowego wydarzenia nie określono wyraźnych kryteriów kwalifikacji poszczególnych incydentów teleinformatycznych jako aktów regulowanych artykułem 5. traktatu waszyngtońskiego, co może rodzić pewne problemy interpretacyjne w przyszłości. Istnieje bowiem możliwość, iż decyzja ta pozostanie jedynie martwym zapisem, formą „straszaka", której praktyczne wykorzystanie może być bardzo trudne ze względu na różnice polityczne między państwami członkowskimi. Z drugiej strony ciekawe rozwiązania przyjęła Unia Europejska, która we właściwym sobie, powolnym i zbiurokratyzowanym rytmie działała na tym polu od początku XXI wieku. Kolejne przedsięwzięcia Komisji Europejskiej w tym wymiarze spotykały się przez lata z niewielkim zainteresowaniem krajów członkowskich, co dowodziło, że sprawy te miały wówczas marginalne znaczenie. Zmieniło się to *de facto* dopiero na początku drugiej dekady XXI wieku, czego wyrazem stała się *Cyber-*

security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Zawarte w niej stwierdzenia o solidarności europejskiej w przypadku poważnego cyberataku miały przełomowy charakter. Niemniej w ramach UE nie udało się, jak dotąd, wypracować bardziej wartościowych mechanizmów praktycznego zwalczania zagrożeń teleinformatycznych. Jeśli chodzi zaś o inne organizacje, takie jak Rada Europy, Szanghajska Organizacja Współpracy, Współpraca Gospodarcza Azji i Pacyfiku czy Organizacja Współpracy Gospodarczej i Rozwoju, to wszystkie w jakimś stopniu uwzględniły w swoich pracach problematykę cyberbezpieczeństwa. Rada Europy zyskała duże znaczenie w tej dziedzinie ze względu na opracowaną przez siebie *Konwencję o cyberprzestępczości* z 2001 roku. Została ona przyjęta przychylnie także poza Starym Kontynentem i stanowiła przez lata wzór tego, w jaki sposób należy przeciwdziałać temu procederowi na szczeblu ponadnarodowym. Niestety ze względu na szereg zarzutów formułowanych m.in. przez Federację Rosyjską nie mogła ona stać się dokumentem obowiązującym globalnie mimo poparcia innych organizacji międzynarodowych. Kontrowersje wokół polityki RE pogłębił protokół dodatkowy do *Konwencji*, którego zapisy zostały sformułowane na tyle szeroko, że można je było interpretować w rozmaity sposób, co budziło zastrzeżenia dotyczące np. wolności słowa w Internecie. Szanghajska Organizacja Współpracy ograniczyła się z kolei wyłącznie do kilku deklaracji oraz projektu umowy międzyrządowej. Ten jednak stał się jednym z nielicznych dokumentów, w których omówiono takie zjawiska, jak cyberwojna czy potencjał cyberprzestrzeni do działań propagandowych. Bez względu na ten fakt w praktyce SCO stała się jedynie narzędziem promocji rosyjskich i chińskich koncepcji rozwoju współpracy międzynarodowej w tym zakresie. Natomiast OECD i APEC, mimo że pozornie nie powinny się tymi zagadnieniami zajmować, wypracowały szereg interesujących propozycji, skupiających się jednak głównie na zjawisku cyberprzestępczości. Na uwagę zasługuje fakt, iż obie blisko ze sobą współdziałały w takich sprawach, jak organizacja warsztatów czy seminariów poświęconych bezpieczeństwu teleinformatycznemu. Niechlubnym przykładem pozostaje Unia Afrykańska, której dotychczasowe wysiłki w tej dziedzinie zakończyły się niepowodzeniem, ponieważ zaproponowane przez nią rozwiązania okazały się wątpliwe z perspektywy ich konsekwencji dla praw człowieka.

Na tym tle należy stwierdzić, iż współpraca międzyrządowa w zakresie zwalczania zagrożeń teleinformatycznych w ostatnich latach staje się coraz intensywniejsza. Niestety nie towarzyszą jej niezbędne inicjatywy zmierzające do wypracowania podstawowych reguł zachowania państw w cyberprzestrzeni. Największą przeszkodą na drodze do urzeczywistnienia idei „cyberpokoju" pozostają odmienne wizje kooperacji w tej dziedzinie formułowane w Waszyngtonie, Moskwie i Pekinie. Żadna z zainteresowanych stron nie jest bez winy, wszystkie traktują bowiem kolejne przedsięwzięcia w środowisku międzynarodowym w sposób instrumentalny. Jak wykazano w pracy, zarówno USA, Chiny,

jak i Rosja stoją za motywowanymi politycznie włamaniami do sieci komputerowych krajów uważanych za wrogie. Co za tym idzie są one zainteresowane regulacją tych kwestii tylko w takim zakresie, jaki nie ograniczy ich własnych zdolności do realizowania swoich celów w cyberprzestrzeni. W tym kontekście można więc odnotować przewagę rywalizacji państw w przestrzeni teleinformatycznej nad przykładami ich skutecznej kooperacji na początku XXI wieku. Dopóki rządy nie znajdą sposobu, aby przezwyciężyć dzielące je w tym względzie różnice, trudno oczekiwać przełomu.

Reasumując, należy podkreślić, że cyberprzestrzeń rzeczywiście stała się na początku XXI wieku nowym wymiarem rywalizacji i współpracy państw. Coraz więcej krajów odwołuje się do cyberataków jako specyficznego środka polityki zagranicznej, osiągając w ten sposób zróżnicowane rezultaty. Tendencjom tym sprzyja impas w międzynarodowej debacie poświęconej bezpieczeństwu teleinformatycznemu, jak również obiektywne cechy samej cyberprzestrzeni. Otwiera to więc zupełnie nowe, wcześniej niespotykane możliwości oddziaływania na innych uczestników stosunków międzynarodowych. Dzięki temu można zaobserwować proces coraz dalej idącej instrumentalizacji tej domeny, przejawiającej się tworzeniem na całym świecie kolejnych jednostek, agencji i dowództw przeznaczonych do ofensywnych i defensywnych działań w sieciach komputerowych. Sytuacja ta ma jednak doniosłe i z gruntu niekorzystne konsekwencje dla całokształtu stosunków międzynarodowych, przede wszystkim oznacza bowiem, że skala ustrukturalizowanych zagrożeń teleinformatycznych będzie coraz większa, o ile nie dojdzie do globalnego porozumienia w tej sprawie. Po drugie — traktowanie ataków komputerowych jako środków polityki zagranicznej może wpływać destabilizująco na stosunki międzypaństwowe oraz stawać się powodem kryzysów i konfliktów przybierających bardziej konwencjonalną formę. Tego typu zapowiedzi formułowały już zresztą Stany Zjednoczone. Po trzecie: pojawiają się obecnie sygnały początku swoistego „wyścigu zbrojeń" w cyberprzestrzeni. Oznacza to, że jeśli będą opracowywane kolejne zaawansowane cyberbronie (takie jak np. *Duqu*), to rządy będą musiały stale podnosić wydatki na ich neutralizację, oznaczającą np. zabezpieczenie infrastruktury krytycznej. Ponadto dominacja rywalizacji nad współpracą w przestrzeni teleinformatycznej może, o czym już wspomniano, osłabić zaufanie do obowiązujących obecnie norm prawa międzynarodowego oraz mechanizmów współpracy politycznej i wojskowej, brak reakcji na te wyzwania wraz z rosnącym uzależnieniem kolejnych sfer życia człowieka od ICT może zatem w przyszłości doprowadzić do trudnych do przewidzenia konsekwencji nie tylko dla bezpieczeństwa państw, lecz także szerzej: dla stabilności całego systemu międzynarodowego.

Bibliografia

Literatura przedmiotu

Abelson P.H., Hammond A.L., 1977: *The Electronic Revolution*. „Science". Vol. 195.

Achenbach J., 1997: *Reality Check*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Adamowski J., Jas M., red., 2004: *Demokracja a nowe środki komunikacji społecznej*. Warszawa.

Adams J., 2001: *The Next World War. Computers Are the Weapons and the Front Line Is Everywhere*. New York.

Adamski A., 2012: *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*. Warszawa.

Agarwal A., Ramana V.V., eds., 2007: *Foundations of E-Government.* Hyderabad.

Akayev A., 1994: *Kyrgyzstan: Central Asia's Democratic Alternative*. „Demokratizatsiia". Vol. 2, no. 1.

Akera A., Aspray W., eds., 2004: *Using History to Teach Computer Science and Related Disciplines*. Washington, D.C.

Alberts D.S., Garstka J.J., Stein F.P., 1999: *Network Centric Warfare. Developing and Leveraging Information Superiority*. Washington, D.C.

Alberts D.S., Papp D.S., Kemp III W.T., 1997: *The Technologies of the Information Revolution*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Alberts D.S., Papp D.S., eds., 1997: *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Aleksandrowicz T.R., Liedel K., 2014: *Społeczeństwo informacyjne — sieć — cyberprzestrzeń. Nowe zagrożenia*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Aleksandrowicz T.R., 2014: *Strategie bezpieczeństwa w cyberprzestrzeni. Cyberwojny*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Alexander K.B., 2007: *Warfighting in cyberspace*. „Joint Forces Quarterly", no. 3.

Alexander K.B., 2012: *An introduction by General Alexander*. „The Next Wave". Vol. 19, no. 4.

Alkassar A., Volkamer M., eds., 2007: *E-voting and Identity*. Bochum.

Anokhin M., Grishin O., 2013: *Energy safety: Politics and diplomacy.* „Przegląd Strategiczny", nr 1.

Armstrong C.K., 2005: *Inter-Korean Relations in Historical Perspective*. „International Journal of Korean Unification Studies". Vol. 14, no. 2.

Arquilla J., Ronfeldt D., 2001: *The Advent of Netwar (Revisited)*. In: Arquilla J., Ronfeldt D., eds., *Networks and Netwars. The Future of Terror, Crime and Militancy*. Santa Monica.

Arquilla J., Ronfeldt D., eds., 2001: *Networks and Netwars. The Future of Terror, Crime and Militancy*. Santa Monica.

Ashmore W.C., 2009: *Impact of Alleged Russian Cyber Attacks*. Fort Leavenworth.

Avila A., 2009: *Underdeveloped ICT areas in Sub-Saharan Africa*. „Informatica Economică". Vol. 13, no. 2.

Balcerowicz B., 2005: *Teorie, koncepcje wojny (i pokoju) po zimnej wojnie*. W: Kuźniar R., red., *Porządek międzynarodowy u progu XXI wieku*. Warszawa.

Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., 2007: *Rocznik Strategiczny 2006/2007*. Warszawa.

Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., 2013: *Rocznik Strategiczny 2012/2013*. Warszawa.

Baldwin D.A., 1997: *The concept of security*. „Review of International Studies", no. 23.

Balmond L., Arcari M., eds., 2012: *La gouvernance globale face aux defis de la sécurité collective*. Napoli.

Bania R., 2012: *Wojny w cyberprzestrzeni — przypadek Iranu*. W: Bania R., Zdulski K., red., *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*. Łódź.

Bania R., Zdulski K., red., 2012: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*. Łódź.

Baocun W., Fei L., 1998: *Information Warfare*. In: Pillsbury M., ed., *Chinese Views of Future Warfare*. Washington, D.C.

Baram G., 2013: *The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case*. „Military and Strategic Affairs". Vol. 5, no. 1.

Barańska B., 2003: *Czy zmierzamy do społeczeństwa informacyjnego*? W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Barcz J., red., 2008: *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*. Warszawa.

Barletta W.A., 2010: *Cyber War or Cyber Terrorism: The Attack on Estonia*. In: Westby J.R., Wegener H., Barletta W., eds., *Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty*. New York.

Bautzmann A., 2012: *Le cyberespace, nouveau champ de bataille?* „Diplomatie. Affaires Stratégiques et Relations Internationales" (février—mars).
Bédar S., 2001: *La Révolution dans les affaires militaires et la „course aux capacités"*. „Forum du désarmament", nr 3.
Bell D., 1960: *The End of Ideology: On the Exhaustion of Political Ideas in the Fifties*. Cambridge.
Bell D., 1999: *The Coming of Post-Industrial Society. The Venture in Social Forecasting*. New York.
Bencsáth B., Pék G., Buttyán L., Félegyházi M., 2012: *The Cousins of Stuxnet: Duqu, Flame and Gauss*. „Future Internet", no. 4.
Berkowitz B., 1997: *Warfare in the Information Age*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Berleur J., Avgerou C., eds., 2005: *Perspectives and Policies on ICT in Society*. New York.
Bieleń S., 2006: *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa.
Bierzanek R., Symonides J., 2002: *Prawo międzynarodowe publiczne*. Warszawa.
Billo C., Chang W., 2004: *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*. Hanover.
Bimber B., 1994: *Three Faces of Technological Determinism*. In: Smith M.R., Marx L., eds., *Does Technology Drive History*. Cambridge.
Blane J.V., ed., 2001: *Cyberwarfare: Terror at a click*. Huntington.
Bobrow D.B., 1997: *Złożoność problematyki braku bezpieczeństwa: implikacje redefinicji pojęcia*. W: Bobrow D.B., Haliżak E., Zięba R., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.
Bobrow D.B., 2000: *Exploiting Open Source Information — Abundance, Value and Intelligence Community Credibility*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.
Bobrow D.B., Haliżak E., Zięba R., 1997: *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.
Bógdał-Brzezińska A., 2009: *Społeczeństwo informacyjne a problemy rozwoju e-government w Polsce*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.
Bógdał-Brzezińska A., Gawrycki M.F., 2003: *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. Warszawa.
Bógdał-Brzezińska A., Gawrycki M.F., 2004: *Rola Internetu wobec procesów demokratyzacji w stosunkach międzynarodowych*. W: Adamowski J., Jas M., red., *Demokracja a nowe środki komunikacji społecznej*. Warszawa.
Bogdański A., 2012: *Na potrzeby sieciocentryczności pola walki*. „Przegląd Wojsk Lądowych", nr 3.
Bolter D.J., 1984: *Turing's Man. Western Culture in the Computer Age*. Chapel Hill.
Boulding K.E., 1953: *The Organizational Revolution: A Study in the Ethics of Economic Organizations*. New York.
Bronk C., 2011: *Blown to Bits. China's War in Cyberspace, August—September 2020*, „Strategic Studies Quarterly" (Spring).

Bryc A., 2006: *Polityka wobec Rosji i innych państw poradzieckich*. W: Zając J., red., *Polityka zagraniczna USA po zimnej wojnie*. Toruń.

Bryc A., 2009: *Rosja w XXI wieku*. Warszawa.

Bryła J., 2000: *Dyplomacja instrumentem polityki zagranicznej państwa.* W: Malendowski W., Mojsiewicz C., red., *Stosunki międzynarodowe.* Wrocław.

Brzeziński Z., 1970: *Between Two Ages. America's Role in the Technetronic Era.* New York.

Bufalini A., 2012: *Les cyber-guerres a la lumière des regles internationales sur l'interdiction du recours à la force*. In: Arcari M., Balmond L., eds., *La gouvernance globale face aux défis de la sécurité collective*. Napoli.

Burnham D., 1983: *The Rise of Computer State*. New York.

Caplan N., 2013: *Cyber War: the Challenge to National Security*. „Global Security Studies". Vol. 4, no. 1.

Carr J., 2010: *Inside Cyber Warfare*. Sebastopol.

Castells M., 2003: *Galaktyka Internetu.* Przeł. T. Hornowski. Poznań.

Chamberlain N., 2013: *Defence Ministers Meeting — June 2013: Keeping NATO Capable.* „NATO Watch Briefing Paper", no. 37.

Chang-Il O., 2010: *The Causes of the Korean War 1950—1953*. „International Journal of Korean Studies". Vol. XIV, no. 2.

Chanlett-Avery E., Rinehart I.E.: *North Korea: U.S. Relations, Nuclear Diplomacy and Internal Situation*. „CRS Report Prepared for Members and Committees of Congress", 15.01.2014.

Chen X., Gao J., Tan W., 2005: *ICT in China: A strong Force to Boost Economic and Social development*. In: Berleur J., Avgerou C., eds., *Perspectives and Policies on ICT in Society*. New York.

Christakis D.A., 2010: *Internet addiction: a 21st century epidemic*? „BMC Medicine", no. 8:61.

Clarke R.A., Knake R.K., 2010: *Cyber War.* New York.

Clarke Z., Clawson J., Cordell M., 2003: *A brief history of hacking.* „Historical Approaches to Digital Media" (November).

Coeira E., 1997: *Medical Informatics*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Cohen-Almagor R., 2011: *Internet History*. „International Journal of Technoethics", no. 2(2).

Colarik A., Janczewski L., 2012: *Establishing Cyber Warfare Doctrine*. „Journal of Strategic Security". Vol. 5, no. 1.

Collins K., 2006: *The Logic of Clan Politics in Central Asia. The Impact on Regime Transformation*. Cambridge.

Comer D.E., 2012: *Sieci komputerowe i intersieci.* Przeł. S. Leszczyński, G. Grudziński, A. Schubert. Gliwice.

Copeland T.E., ed., 2000: *The Information Revolution and National Security*. Carlisle.

Cordesman A.H., Cordesman J.G., 2001: *Cyber-threats, Information Warfare and Critical Infrastructure Protection. Defending the U.S. Homeland*. Washington, D.C.

Cornish P., Livingstone D., Clemente D., Yorke C., 2010: *On Cyber Warfare*. „A Chatham House Report" (November).

Creedon M.R., 2012: *Space and Cyber. Shared Challenges, Shared Opportunities*. „Strategic Studies Quarterly". Vol. 6, no. 1.

Cutts A., 2009: *Warfare and the Continuum of Cyber Risks: A Policy Perspective*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare.* Amsterdam.

Czaputowicz J., 2006: *Bezpieczeństwo w teoriach stosunków międzynarodowych*. W: Żukrowska K., Grącik M., red., *Bezpieczeństwo międzynarodowe. Teoria i praktyka*. Warszawa.

Czaputowicz J., 2012: *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*. Warszawa.

Czebotar Ł., 2013: *Strategia Stanów Zjednoczonych wobec problemu bezpieczeństwa cyberprzestrzeni*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna.* Warszawa.

Czermiński A., Grzybowski M., Ficoń K., 1999: *Podstawy organizacji i zarządzania*. Gdynia.

Cziomer E., 2005: *Polityka zagraniczna państwa*. W: Cziomer E., Zyblikiewicz L., *Zarys współczesnych stosunków międzynarodowych.* Warszawa.

Cziomer E., Zyblikiewicz L., 2005: *Zarys współczesnych stosunków międzynarodowych*. Warszawa.

Czornik K., 2011: *Irak w polityce zagranicznej Stanów Zjednoczonych w okresie pozimnowojennym*. Katowice.

Czornik K., 2012: *Bliski Wschód w polityce zagranicznej Stanów Zjednoczonych w latach 1945—2012*. Katowice.

Czosseck C., Geers K., eds., 2009: *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.

Czosseck C., Klein G., Leder F., 2011: *Botnets — Setting Up and Taking Down Botnets*. In: Czosseck C., Tyugu E., Wingfield T., eds., *2011 3rd International Conference on Cyber Conflict*. Tallin.

Czosseck C., Ottis R., Ziolkowski K., eds., 2012: *4th International Conference on Cyber Conflict*. Tallin.

Czosseck C., Tyugu E., Wingfield T., eds., 2011: *2011 3rd International Conference on Cyber Conflict*. Tallin.

Dawidziuk P., Łącki B., Stolarski M.P., 2009: *Sieć Internet — znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

de Haas M., 2007: *The Shanghai Cooperation Organisation and the OSCE: Two of a kind?* „Helsinki Monitor: Security and Human Rights", no. 3.

de Haas M., van der Putten F.P., 2007: *The Shanghai Cooperation Organisation. Towards a full-grown security alliance?* Hague.

Deibert R., 2013: *Black Code: Inside the Battle for Cyberspace*. Toronto.

Delpech T., 2001: *L'Arms Control est-il soluble dans la RMA?* „Forum du désarmament", no. 3.

Denning D.E., 2011: *Cyber Conflict as an Emergent Social Phenomenon.* In: Holt T.J., Schell B.H., eds., *Corporate Hacking and Technology — Driven Crime: Social Dynamics and Implications*. Hershey.

Devost M.G., Houghton B.K., Pollard N.A., 1997: *Information Terrorism: Can You Trust Your Toaster*? In: Neilson R.E., ed., *Sun Tzu and Information Warfare*. Washington, D.C.

Dobroczyński M., Stefanowicz J., 1984: *Polityka zagraniczna*. Warszawa.

Doktorowicz K., 2003: *Społeczności wirtualne — cyberprzestrzeń w poszukiwaniu utraconych więzi*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Dowty A., 1999: *Israeli Foreign Policy and the Jewish Question*. „Middle East Review of International Affairs". Vol. 3, no. 1.

Drake W., 2000: *Multilateral Institutions in the Global Information Economy*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.

Drzyzga P., red., 2007: *Nowe media a tradycyjne środki przekazu*. Kraków.

Dunn M.A., 2001: *The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method*. „Information & Security". Vol. 7.

Dunn M.A., 2002: *Information Age Conflicts. A Study of the Information Revolution and a Changing Operating Environment*. „Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung", no. 64.

Dunn-Cavelty M.A., 2007: *Critical information infrastructure: vulnerabilities, threats and responses*. „Disarmament Forum", no. 3.

Dunn-Cavelty M.A., 2008: *Cyber-Security and Threat Politics*. New York.

Dunn-Cavelty M.A., 2012: *The militarisation of cyber security as a source of global tension*. In: Möckli D., ed., *Strategic Trends 2012*. Zurich.

Durkalec J., 2007: *Rola broni atomowej w polityce zagranicznej w XXI wieku*. W: Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., *Rocznik Strategiczny 2006/2007*. Warszawa.

Dyduch J., 2011: *Polityka zagraniczna Izraela: kontynuacja i zmiana*. W: Łoś-Nowak T., red., *Polityka zagraniczna. Aktorzy — potencjały — strategie.* Warszawa.

Dzisiów-Szuszczykiewicz A., 2012: *Regionalna rywalizacja o Syrię*. „Bezpieczeństwo Narodowe", nr 2.

Dziwisz D., 2011: *Cyberbezpieczeństwo — nowy priorytet strategii obrony Stanów Zjednoczonych*. „Sprawy Międzynarodowe", nr 3.

Dziwisz D., 2013a: *Cyberbezpieczeństwo infrastruktury krytycznej — priorytet strategii obrony USA?* W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.

Dziwisz D., 2013b: *Rozmowa z dr. Martinem C. Libickim, ekspertem ds. bezpieczeństwa*. „Bezpieczeństwo Narodowe", nr 2.

Eidintas A., Bumblauskas A., Kulakauskas A., Tamošaitis M., 2013: *Historia Litwy*. Wilno.

Erice Declaration of Principles for Cyber Stability and Cyber Peace. In: Touré H.I., ed., *The Quest for Cyber Peace*. Geneva 2011.

Eriksson J., Giacomello G., 2006: *The Information Revolution, Security, and International Relations: (IR)relevant Theory?* „International Political Science Review". Vol. 27, no. 3.

Even S., Siman-Tov D., 2012: *Cyber Warfare: Concepts and Strategic Trends*. Tel Aviv.
Ezell S., Andes S., 2010: *ICT R&D Policies. An International Perspective*. „IEEE Internet Computing". Vol. 14, no. 4.
Fajgielski P., 2013: *Rozwój technologii informacyjnych i komunikacyjnych oraz związanych z nimi zagrożeń — wybrane aspekty prawne*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.
Farivar C., 2009: *A Brief Examination of Media Coverage of Cyberattacks (2007 — Present)*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare.* Amsterdam.
Feakin T., 2012: *Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities*. „International Journal of Korean Unification Studies". Vol. 22, no. 2.
Fitri N., 2011: *Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the Global Changing*. „Online Journal of Communication and Media Technologies", no. 2.
Fogelman M., 1997: *Freedom and Censorship in the Emerging Electronic Environment*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences.* Fort McNair.
Foltz A.C., 2012: *Stuxnet, Schmitt Analysis, and the Cyber „Use-of-force" Debate*. „Joint Force Quarterly". Vol. 67, no. 4.
Foster-Carter A., 2007: *North Korea — South Korea Relations: Summit Success?* „Comparative Connections. A Quarterly E-Journal on East Asian Bilateral Relations". October.
Fulmański P., Sobieski Ś., 2004: *Wstęp do informatyki*. Łódź.
Gacek Ł., 2009: *Chińska koncepcja bezpieczeństwa międzynarodowego*. W: Olszewski P., Kapuśniak T., Lizak W., red., *Bezpieczeństwo międzynarodowe. Wyzwania i zagrożenia XXI wieku*. Radom.
Gagnon B., 2009: *Informatique et cyberterrorisme*. In: Leman-Langlois S., Brodeur J.-P., eds., *Terrorisme et antiterrorisme au Canada*. Montréal.
Gała K., 2009: *Wpływ korporacji transnarodowych na wdrażanie koncepcji bezpieczeństwa ludzkiego*. W: Olszewski P., Kapuśniak T., Lizak W., red., *Bezpieczeństwo międzynarodowe. Wyzwania i zagrożenia XXI wieku*. Radom.
Gartzke E., 2013: *The Myth of Cyberwar. Bringing War on the Internet Back Down to Earth*. „International Security". Vol. 38, no. 2.
Gasparini-Alves P., ed., 1997: *Increasing Access to Information Technology for International Security. Forging Cooperation Among Research Institutes*. New York, Geneva.
Gawrysiak P., 2008: *Cyfrowa rewolucja*. Warszawa.
Geers K., 2011: *Strategic Cyber Security*. Tallin.
Geers K., 2014: *Pandemonium: Nation States, National Security, and the Internet*. „The Tallin Papers". Vol. 1, no. 1.
Gerber T.P., Conley H.A., Moore L., 2011: *Estonia and Russia through a Three-Way Mirror*. „PONARS Eurasia Policy Memo", no. 145.
German T., 2006: *Abkhazia and South Ossetia: Collision of Georgian and Russian Interests*. „Russie.Nei.Visions", no 11.

German T.C., 2006: *Le conflit en Ossétie-du-Sud: la Géorgie contre la Russie*. „Politique étrangère", no. 1.
Gibson W., 1984: *Neuromancer*. New York.
Giddens A., 1975: *The Class Structure of the Advanced Societies*. New York.
Giles K., 2011: *„Information Troops" — A Russian Cyber Command?* In: Czosseck C., Tyugu E., Wingfield T., eds., *2011 3rd International Conference on Cyber Conflict*. Tallin.
Giles K., 2012: *Russia's Public Stance on Cyberspace Issues*. In: Czosseck C., Ottis R., Ziolkowski K., eds., *4th International Conference on Cyber Conflict*. Tallin.
Glabus E.M., 2000: *Metaphors and Modern War: Biological, Computer and Cognitive Viruses*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.
Goban-Klas T., 2003: *Ontologia Internetu*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość?* Kraków.
Goban-Klas T., Sienkiewicz P., 1999: *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków.
Gogolashvili K., ed., 2011: *Russia and Georgia: Searching the Way Out*. Tbilisi.
Gogołek W., 2004: *Demokracja w sieci*. W: Adamowski J., Jas M., red., *Demokracja a nowe środki komunikacji społecznej*. Warszawa.
Green J.L., 1988: *The space physics analysis network*. „Computer Physics Communications". Vol. 49, no. 1.
Griffin E., 2008: *A first look at communication theory.* Columbus.
Grochmalski P., 2003: *Rosja — Czeczenia. Dwie ostatnie imperialne wojny XX wieku*. W: Malendowski W., red., *Zbrojne konflikty i spory międzynarodowe u progu XXI wieku. Analiza problemów i studia przypadku*. Wrocław.
Grosse T.G., 2013: *Erozja systemu geopolitycznego USA. Rola liberalizacji rynków finansowych*. „Studia Polityczne", nr 31.
Grzelak A., 2008: *Reforma Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości*. W: Barcz J., red., *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*. Warszawa.
Grzelak M., 2013: *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*. „Bezpieczeństwo Narodowe", nr 2.
Guisnel J., 1997a: *Cyberwars. Espionage on the Internet*. New York—London.
Guisnel J., 1997b: *Guerres dans le cyberespace. Services secrets et Internet*. Paris.
Gulbas K., 2012: *Wyzwania dla wojsk łączności*. „Przegląd Wojsk Lądowych", nr 3.
Gupta K.D., Joshi J., 2012: *Methodogical and Operational deliberations in Cyber attack and Cyber exploitation*. „International Journal of Advanced Research in Computer Science and Software Engineering", no. 11 (November).
Haber L.H., red., 2001: *Mikrospołeczność informacyjna*. Kraków.
Haber L.H., red., 2003: *Społeczeństwo informacyjne — wizja czy rzeczywistość?* Kraków.
Haigh T., 2004: *The History of Computing: An Introduction for the Computer Scientist*. In: Akera A., Aspray W., eds., *Using History To Teach Computer Science and Related Disciplines*. Washington, D.C.

Haliżak E., 1997: *Ekonomiczny wymiar bezpieczeństwa narodowego i międzynarodowego*. W: Bobrow D.B., Haliżak E., Zięba R., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.

Haliżak E., 2006: *Współpraca międzynarodowa*. W: Haliżak E., Kuźniar R., red., *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.

Haliżak E., 2013a: *Poziomy analizy w nauce o stosunkach międzynarodowych*. W: Haliżak E., Pietraś M., red., *Poziomy analizy stosunków międzynarodowych*. Warszawa.

Haliżak E., 2013b: *Region Azji i Pacyfiku — logika geoekonomii i geopolityki*. W: Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., *Rocznik Strategiczny 2012/2013*. Warszawa.

Haliżak E., Kuźniar R., red., 2006: *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.

Haliżak E., Pietraś M., red., 2013: *Poziomy analizy stosunków międzynarodowych*. Warszawa.

Haltmaier J., 2013: *Challenges for the Future of Chinese Economic Growth*. „International Finance Discussion Papers", no. 1072 (January).

Hampson N.C.N., 2012: *Hacktivism: A New Breed of Protest in a Network World*. „Boston College International and Comparative Law Review", no. 2.

Hansman S., Hunt R., 2005: *A taxonomy of network and computer attacks*. „Computers & Security", no. 1.

Hare F., 2009: *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.

Harris S., Harper A., Eagle C., Ness J., 2008: *Grey Hat Hacking. The Ethical Hacker's Handbook*. New York, Chicago.

Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J., 2012: *The Law of Cyber-Attack*. „California Law Review". Vol. 100.

Heinl C.H., 2012: *Preventing a Digital Pearl Harbor: Panetta's Key Recommendations*. „RSIS Commentaries", no. 209.

Heintschel von Heinegg W., 2012: *Legal Implications of Territorial Sovereignty in Cyberspace*. In: Czosseck C., Ottis R., eds., *2012 4th International Conference on Cyber Conflict*. Tallin.

Heintschel von Heinegg W., 2013: *Territorial Sovereignty and Neutrality in Cyberspace*. „International Law Studies". Vol. 89.

Herz J.H., 1959: *Idealist Internationalism and Security Dilemma*. „World Politics", no. 2.

Herzog S., 2011: *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. „Journal of Strategic Security", no. 2.

Hess P., ed., 2001: *Cyberterrorism and information war*. New Delhi.

Hetmański M., 2003: *Nowe zdolności poznawcze w systemach informatycznych*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Hildreth S.A., 2002: *Cyberwarfare*. In: Blane J.V., ed., *Cyberwarfare: Terror at a Click*. New York.

Hjortdal M., 2011: *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*. „Journal of Strategic Studies". Vol. 4, no. 2.

Hollis D.: *Cyberwar Case Study: Georgia 2008*. „Small Arms Journal", 06.01.2011.
Holsti K.J., 1967: *International Politics: A Framework for Analysis*. New Jersey.
Holt T.J., Schell B.H., eds., 2011: *Corporate Hacking and Technology — Driven Crime: Social Dynamics and Implications*. Hershey.
Horan T.A., Grönlund Å., 2004: *Introducing e-GOV: History, definitions and issues*. „Communications of the Association for Information Systems". Vol. 15.
Huber P., 1997: *Cyberpower*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Hundley R.O., Anderson R.H., Bikson T.K., Neu C.R., 2003: *The Global Course of the Information Revolution. Recurring Themes and Regional Variations*. Santa Monica.
Huskey E., 2008: *Foreign Policy in a Vulnerable State: Kyrgyzstan as Military Entrepot Between the Great Powers*. „China and Euroasia Forum Quarterly". Vol. 6, no. 4.
Infrastructure Protection. Defending the U.S. Homeland. Washington, D.C. 2001.
Isenberg D., Meridian D., 2000: *An Electronic Pearl Harbor? Not Likely*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.
Jain Palvia S.C., Sharma S.S., 2007: *E-Government and E-Governance: Definitions/ Domain Framework and Status Around the World*. In: Agarwal A., Ramana V.V., eds., *Foundations of E-Government*. Hyderabad.
Janczak J., Nowak A., 2013: *Bezpieczeństwo informacyjne. Wybrane problemy*. Warszawa.
Jarczewska A., 2013: *Stany Zjednoczone — w Białym Domu bez zmian.* W: Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., *Rocznik Strategiczny 2012/2013*. Warszawa.
Jawasreh M., 2003: *Proces pokojowy na Bliskim Wschodzie*. W: Malendowski W., red., *Zbrojne konflikty i spory międzynarodowe u progu XXI wieku*. Wrocław.
Jeran A., 2003: *Mit Internetu jako miejsca poszukiwania informacji*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość?* Kraków.
Jordan T., 2011: *Hakerstwo*. Przeł. T. Płudowski. Warszawa.
Jordan T., Taylor P., 2004: *Hacktivism and Cyberwars: Rebels With a Cause?* London.
Joubert V., 2012: *Five years after Estonia's cyber attacks: lessons learned for NATO?* „NATO Defense College Research Paper", no. 76.
Kaczmarski M., 2006: *Polityka wobec Azji Wschodniej*. W: Zając J., red., *Polityka zagraniczna USA po zimnej wojnie*. Toruń.
Kallberg J., 2012: *Designer Satellite Collisions from Covert Cyber War*. „Strategic Studies Quarterly". Vol. 6, no. 1.
Kambil A., 1997: *Electronic Commerce: Implications of the Internet for Business Practice and Strategy*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Kanuck S., 2009: *Sovereign Discourse on Cyber Conflict under International Law*. „Texas Law Review". Vol. 88.
Kanwal G., 2009: *China's Emerging Cyber War Doctrine*. „Journal of Defence Studies". Vol. 3, no. 3.
Kapuśniak T., red., 2011: *Wspólnota Niepodległych Państw: fragmegracja — bezpieczeństwo — konflikty etniczne*. Lublin.

Kasekamp A., ed., 2005: *The Estonian Foreign Policy Yearbook 2005*. Tallin.
Katz I.R., Smith-Macklin A., 2007: *Information and Communication Technology (ICT) Literacy: Integration and Assessment in Higher Education*. „Journal of Systemics, Cybernetics and Informatics". Vol. 5, no. 4.
Kenway J., Bullen E., Fahey J., Robb S., 2006: *Haunting the Knowledge Economy*. New York.
Kępa L., 2014: *Ochrona danych osobowych w praktyce*. Warszawa.
Kim Y., Eom G.-H., 2008: *The Geopolitics of Caspian Oil: Rivalries of the US, Russia, and Turkey in the South Caucasus*. „Global Economic Review", no. 1.
Kitler W., 2002: *Obrona narodowa III RP. Pojęcie. Organizacja. System*. „Zeszyty Naukowe AON". Warszawa.
Kiwerska J., 2012: *Stany Zjednoczone w świecie zróżnicowanych potęg*. „Przegląd Zachodni", nr 4.
Kjaerland M., 2005: *A classification of computer security incidents based on reported attack data*. „Journal of Investigative Psychology and Offender Profiling", nr 2.
Kjaerland M., 2006: *A taxonomy and comparison of computer security incidents from the commercial and government sectors*. „Computers & Security", no. 7.
Kołodziej E.A., 1997: *Bezpieczeństwo międzynarodowe po zimnej wojnie: od globalizacji do regionalizacji*. W: Bobrow D.B., Haliżak E., Zięba R., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.
Kondrakiewicz D., 2013: *Metody pomiaru siły państwa w stosunkach międzynarodowych*. W: Haliżak E., Pietraś M., red., *Poziomy analizy stosunków międzynarodowych*. Warszawa.
Korns S.W., Kastenberg J.E.: *Georgia's Cyber Left Hook*. „Parameters". Vol. 38, no. 4/2008-09
Kosmynka S., 2013: *Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.
Kostecki W., 1988: *Polityka zagraniczna. Teoretyczne podstawy badań*. Warszawa.
Kostecki W., 2013: *Poziomy analizy polityki zagranicznej*. W: Haliżak E., Pietraś M., red., *Poziomy analizy stosunków międzynarodowych*. Warszawa.
Kowalkowski S., 2011: *Bezpieczeństwo publiczne — pojęcie, charakter i uwarunkowania*. W: Kowalkowski S., red., *Niemilitarne zagrożenia bezpieczeństwa publicznego*. Warszawa.
Kowalkowski S., red., 2011: *Niemilitarne zagrożenia bezpieczeństwa publicznego*. Warszawa.
Kramer F.D., Starr S., Wentz L.K., eds., 2009: *Cyberpower and National Security*. Washington, D.C.
Kshetri N., 2005: *Pattern of global cyber war and crime: A conceptual framework*. „Journal of International Menagement". Vol. 11.
Kuehl D.T., 2009: *From Cyberspace to Cyberpower: Defining the Problem*. In: Kramer F.D., Starr S., Wentz L.K., eds., *Cyberpower and National Security.* Washington, D.C.
Kuhn M.G., Anderson R.J., 1998: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*. „Lecture Notes in Computer Science". Vol. 1525.

Kukułka J., 1994: *Narodziny nowych koncepcji bezpieczeństwa*. W: Kukułka J., red., *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*. Warszawa.
Kukułka J., 1995: *Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski*. „Wieś i Państwo", nr 1.
Kukułka J., 2003: *Wstęp do nauki o stosunkach międzynarodowych*. Warszawa.
Kukułka J., red., 1992: *Polityka zagraniczna państwa*. Warszawa.
Kukułka J., red., 1994: *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*. Warszawa.
Kulesa Ł., 2014: *Światełko w tunelu? Szanse na całościowe porozumienie w sprawie irańskiego programu nuklearnego*. „Biuletyn PISM", nr 7(1119).
Kurowski W., 2006: *Pojęcie organizacji przestępczej i przestępczości zorganizowanej*. „Prokuratura i Prawo", nr 1.
Kuźniar R., 2006a: *Bezpieczeństwo w stosunkach międzynarodowych*. W: Haliżak E., Kuźniar R., red., *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.
Kuźniar R., 2006b: *Stosunki międzynarodowe — istota, uwarunkowania, badanie*. W: Haliżak E., Kuźniar R., red., *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.
Kuźniar R., 2012a: *Tradycyjne zagrożenia dla bezpieczeństwa państwa*. W: Kuźniar R., Balcerowicz B., Bieńczyk-Missala A., Grzebyk P., Madej M., Pronińska K., Sułek M., Tabor M., Wojciuk A., *Bezpieczeństwo międzynarodowe*. Warszawa.
Kuźniar R., 2012b: *Wstęp*. W: Kuźniar R., Balcerowicz B., Bieńczyk-Missala A., Grzebyk P., Madej M., Pronińska K., Sułek M., Tabor M., Wojciuk A., *Bezpieczeństwo międzynarodowe*. Warszawa.
Kuźniar R., red., 2005: *Porządek międzynarodowy u progu XXI wieku*. Warszawa.
Kuźniar R., Balcerowicz B., Bieńczyk-Missala A., Grzebyk P., Madej M., Pronińska K., Sułek M., Tabor M., Wojciuk A., 2012: *Bezpieczeństwo międzynarodowe*. Warszawa.
Kyrgyzstan Country Profile. „Central Asia Executive Summary Series", no. 2/2009.
Laasme H., 2011: *Estonia: Cyber Window into the Future of NATO*. „Joint Force Quarterly", no. 63.
Lafargue F., 2005: *États-Unis, Indie, Chine: rivalités pétrolières en Afrique*. „Afrique Contemporaine", no. 4.
Lai R., Rahman S., 2012: *Analytic of China cyberattack*. „The International Journal of Multimedia & Its Applications". Vol. 4, no. 3.
Lakomy M., 2010a: *Geopolityczne następstwa wojny gruzińsko-rosyjskiej*. „Przegląd Zachodni", nr 4.
Lakomy M., 2010b: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe — International Relations", nr 3—4.
Lakomy M., 2011: *Arab Spring and New Media*. In: Przybylska-Maszner B., ed., *The Arab Spring*. Poznań.
Lakomy M., 2011a: *Cyberwojna jako rzeczywistość XXI wieku*. „Stosunki Międzynarodowe — International Relations", nr 3—4.
Lakomy M., 2011b: *Stany Zjednoczone w polityce zagranicznej Francji w okresie pozimnowojennym*. Toruń.

Lakomy M., 2012: *Cyberzagrożenia na początku XXI wieku*. „Przegląd Zachodni", nr 4.
Lakomy M., 2013: *Demokracja 2.0. Interakcja polityczna w nowych mediach*. Kraków.
Lakomy M., 2013a: *Organizacja Narodów Zjednoczonych wobec wyzwań dla bezpieczeństwa teleinformatycznego*. „Gdańskie Studia Międzynarodowe". T. 11, nr 1—2.
Lakomy M., 2013b: *Polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego*. „Przegląd Zachodni", nr 4.
Lakomy M., 2013c: *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego — zarys problemu*. „Rocznik Integracji Europejskiej", nr 7.
Lakomy M., 2013d: *Zagrożenia dla bezpieczeństwa teleinformatycznego państw — przyczynek do typologii*. „E-Politikon", nr 6.
Lamberton D.M., 1974: *Information Revolution*. „The Annals of the American Academy of Political and Social Sciences". Vol. 412.
Lasoń W., Walecki P., Trąbka J., 2003: *Telemedyczne bazy danych — teoria i praktyka*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.
Latoszek E., 2007: *Integracja europejska. Mechanizmy i wyzwania*. Warszawa.
Leder F., Werner T., Martini P., 2009: *Proactive Botnet Countermeasures An Offensive Approach*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.
Leiner B.M., Cerf V.G., Clark D.D., Kahn R.E., Kleinrock L., Lynch D., Postel J., Roberts L.G., Wolff S.S., 1997: *The Past and Future of History of the Internet*. „Communications of the ACM". Vol. 40, no. 2.
Lekowski M., 2011: *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*. „Bezpieczeństwo Narodowe", nr 3.
Leman-Langlois S., Brodeur J.-P., eds., 2009: *Terrorisme et antiterrorisme au Canada*. Montréal.
Leszczyńska M., 2011: *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej*. W: Woźniak M.G., red., *Nierówności społeczne a wzrost gospodarczy. Społeczeństwo informacyjne — regionalne aspekty rozwoju*. Rzeszów.
Leszczyński M., 2011: *Bezpieczeństwo społeczne a współczesne państwo*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 2.
Levy S., 2010: *Hackers: Heroes of the Computer Revolution*. Sebastopol.
Liang Q., Xiangsui W., 1999: *Unrestricted Warfare*. Beijing.
Libicki M.C., 2013: *The Cyberwar challenge to NATO*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.
Libicki M.C., 2007: *Conquest in Cyberspace. National Security and Information Warfare*. New York.
Lichocki E., 2011: *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*. W: Liedel K., red., *Transsektorowe obszary bezpieczeństwa narodowego*. Warszawa.
Liderman K., 2009: *Analiza ryzyka i ochrona informacji w systemach komputerowych*. Warszawa.
Liderman K., 2012: *Bezpieczeństwo informacyjne*. Warszawa.

Liedel K., 2011: *Bezpieczeństwo informacyjne państwa*. W: Liedel K., red., *Transsektorowe obszary bezpieczeństwa narodowego*. Warszawa.

Liedel K., 2014: *Kształtowanie zdolności ofensywnych w cyberprzestrzeni*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Liedel K., red., 2011: *Transsektorowe obszary bezpieczeństwa narodowego*. Warszawa.

Liedel K., Piasecka P., 2011: *Wojna cybernetyczna — wyzwanie XXI wieku*. „Bezpieczeństwo Narodowe", nr 1.

Liedel K., Piasecka P., Aleksandrowicz T.R., red., 2014: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Liles S., Rogers M., Larson D., Dietz J.E., 2012: *Applying Traditional Military Principles to Cyber Warfare*. In: Czosseck C., Ottis R., Ziolkowski K., eds., *2012 4th International Conference on Cyber Conflict*. Tallin.

Lizak W., 1997: *Wpływ czynnika etnicznego na bezpieczeństwo międzynarodowe*. W: Bobrow D.B., Haliżak E., Zięba R., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.

Lizak W., 2007: *Liban — wojna Izraela z Hizb'ullahem*. W: Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., *Rocznik Strategiczny 2006/2007*. Warszawa.

Łebkowska J., 2011: *Bezpieczeństwo — teoretyczny wymiar ponadczasowej wartości*. „Przegląd Strategiczny", nr 1.

Łopińska A., 2012: *Chiny w XXI wieku — potęga regionalna czy mocarstwo światowe*? „Przegląd Zachodni", nr 4.

Łoś-Nowak T., 2008: *Polityka zagraniczna*. W: Łoś-Nowak T., red., *Współczesne stosunki międzynarodowe*. Wrocław.

Łoś-Nowak T., 2011: *Polityka zagraniczna — stałe i zmienne komponenty procesu formułowania i realizacji*. W: Łoś-Nowak T., red., *Polityka zagraniczna. Aktorzy — potencjały — strategie*. Warszawa.

Łoś-Nowak T., red., 2008: *Współczesne stosunki międzynarodowe*. Wrocław.

Łoś-Nowak T., red., 2010: *Współczesne stosunki międzynarodowe*. Wrocław.

Łoś-Nowak T., red., 2011: *Polityka zagraniczna. Aktorzy — potencjały — strategie*. Warszawa.

Lu C., Jen W., Chang W., Chou S., 2006: *Cybercrime & Cybercriminals: An Overview of the Taiwan Experience*. „Journal of Computers". Vol. 1, no. 6.

Made V., 2005: *Estonian — Russian relations in the context of the international system*. W: Kasekamp A., ed., *The Estonian Foreign Policy Yearbook 2005*. Tallin.

Madej M., 2005: *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego — próba teoretycznej konceptualizacji*. W: Kuźniar R., red., *Porządek międzynarodowy u progu XXI wieku*. Warszawa.

Madej M., 2009: *Rewolucja informatyczna — istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Madej M., Terlikowski M., 2009: *Wprowadzenie*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Madej M., Terlikowski M., red., 2009: *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Madnick S., Choucri N., Camiña S., Woon W.L., 2012: *Towards better understanding Cybersecurity: or are „Cyberspace" and „Cyber Space" the same?* „Working Paper CISL" (November).

Mahoney M.S., 1988: *The History of Computing in the History of Technology*. „Annals of the History of Computing", no. 10.

Malendowski W., 2000: *Pokój i bezpieczeństwo międzynarodowe*. W: Malendowski W., Mojsiewicz C., red., *Stosunki międzynarodowe*. Wrocław.

Malendowski W., red., 2003: *Zbrojne konflikty i spory międzynarodowe u progu XXI wieku. Analiza problemów i studia przypadku*. Wrocław.

Malendowski W., Mojsiewicz C., Czachór Z., Bryła J., 2007: *Leksykon współczesnych międzynarodowych stosunków politycznych*. Wrocław.

Malendowski W., Mojsiewicz C., red., 2000: *Stosunki międzynarodowe*. Wrocław.

Marszałek-Kawa J., 2011: *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*. W: Łoś-Nowak T., red., *Polityka zagraniczna. Aktorzy — potencjały — strategie*. Warszawa.

Martin J., Norman A.R.D., 1970: *The Computerized Society: an Appraisal of the Impact of Computers on Society Over the Next Fifteen Years*. New Jersey.

Matera P., 2012a: *Relacje transatlantyckie w czasie prezydentury Baracka Obamy*. „Przegląd Zachodni", nr 4.

Matera P., 2012b: *Rywalizacja gospodarcza Stanów Zjednoczonych z Chinami w Afryce Subsaharyjskiej w XXI wieku*. „Stosunki Międzynarodowe — International Relations", nr 2.

Matray J.I., 2013: *The Failure of the Bush Administration's North Korea Policy: A Critical Analysis*. „International Journal of Korean Studies". Vol. XVII, no. 1.

Mazarr M.J., 1994: *The Revolution in Military Affairs. A Framework for Defense Planning*. Carlisle.

Mazur M., 1999: *Cybernetyka i charakter*. Warszawa.

McAfee J., Haynes C., 1989: *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*. New York.

McLuhan M., 2003: *Understanding Media: The Extensions of Man*. Berkeley.

McLuhan M., Fiore Q., 1968: *War and Peace in the Global Village: an inventory of some of the current spastic situations that could be eliminated by more feedforward*. New York.

Mehan J.E., 2008: *CyberWar, CyberTerror, CyberCrime. A Guide to the Role of Standards in an Environment of Change and Danger*. Cambridge.

Mehlinger H.D., 1997: *School Reform in the Information Age*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Melnitzky A., 2012: *Defending America against Chinese Cyber Espionage Through the Use of Active Defenses*. „Cardozo Journal of International and Comparative Law". Vol. 20.2 (Winter).

Messner Z., 1971: *Informacja ekonomiczna a zarządzanie przedsiębiorstwem*. Warszawa.

Metz S., 2000: *Lessons from Military Experience: The U.S. Military and the IR: The Pitfalls of Uneven Adaptation*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.

Michałowska G., 1997: *Bezpieczeństwo kulturowe w warunkach globalizacji procesów społecznych*. W: Bobrow D.B., Haliżak E., Zięba R., red., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa.

Miller R.A., Kuehl D.T., 2009: *Cyberspace and the „First Battle" in 21st-century War*. „Defense Horizons" (September).

Milone M.G., 2002: *Hacktivism: Securing the National Infrastructure*. „The Business Lawyer". Vol. 58, no. 1.

Miszczak M., 2008: *Reforma Wspólnej Polityki Zagranicznej i Bezpieczeństwa*. W: Barcz J., red., *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*. Warszawa.

Mojsiewicz C., 2000: *Co wpływa na bezpieczeństwo i suwerenność państw?* W: Malendowski W., Mojsiewicz C., red., *Stosunki międzynarodowe*. Wrocław.

Molander R.C., Riddile A.S., Wilson P.A., 1996: *Strategic Information Warfare. A New Face of War*. Santa Monica.

Murray W., 1997: *Thinking about Revolutions in Military Affairs*. „Joint Force Quarterly" (Summer).

Myszczyn J., Myszczyn W., 2003: *Informacja — czwartym czynnikiem produkcji*. W: Piech K., Szczodrowski G., red., *Przemiany i perspektywy polskich przedsiębiorstw w dobie integracji z Unią Europejską*. Warszawa.

Nachev A., 2000: *Electromagnetic Radiation and the Computer Data Security Problem*. „Information & Security". Vol. 4.

Nazario J., 2009: *Politically Motivated Denial of Service Attacks*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.

Neilson R.E., ed., 1997: *Sun Tzu and Information Warfare*. Washington, D.C.

Nekrašas E., 2004: *Lithuanian Foreign Policy: Achievements, Concepts and Predicaments*. „Lithuanian Foreign Policy Review", no. 1—2.

Niezgoda M., 2003: *Społeczeństwo informacyjne w perspektywie socjologicznej: idea czy rzeczywistość?* W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Nikolov E., 2000: *Contemporary Trends in the Development of Information Security and Computer Virology*. „Information & Security". Vol. 4.

Noor E., 2011: *The Problem with Cyber Terrorism*. „SEARCCT's Selection of Articles", no. 2.

Nowak E., Nowak M., 2011: *Zarys teorii bezpieczeństwa narodowego*. Warszawa.

Nowiak J., 2000: *Czym jest polityka zagraniczna*? W: Malendowski W., Mojsiewicz C., red., *Stosunki międzynarodowe*. Wrocław.

O'Connell M.E., 2012: *Cyber Security without Cyber War*. „Journal of Conflict & Security Law". Vol. 17, no. 2.

Ociepka B., 2013: *Miękka siła państwa i jej pomiar — czy to ma sens?* W: Haliżak E., Pietraś M., red., *Poziomy analizy stosunków międzynarodowych*. Warszawa.

Olszewski P., Kapuśniak T., Lizak W., red., 2009: *Bezpieczeństwo międzynarodowe. Wyzwania i zagrożenia XXI wieku*. Radom.

Pacek B., Hoffmann R., 2013: *Działania sił zbrojnych w cyberprzestrzeni*. Warszawa.
Paget F., 2012: *Hacktivism. Cyberspace has become the new medium for political voices*. „McAfee Labs White Paper".
Papp D.S., Alberts D.S., Tuyahov A., 1997: *Historical Impacts of Information Technologies: Overview*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Pawlikowska I., 2005: *Bezpieczeństwo jako cel polityki zagranicznej państwa*. W: Zięba R., red., *Wstęp do teorii polityki zagranicznej państwa*. Toruń.
Piasecka P., 2011: *Zagrożenia ładu i bezpieczeństwa międzynarodowego we współczesnym świecie*. W: Liedel K., red., *Transsektorowe obszary bezpieczeństwa narodowego*. Warszawa.
Piasecka P., 2014: *Armie przyszłości — wojna sieciocentryczna*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.
Piech K., Szczodrowski G., red., 2003: *Przemiany i perspektywy polskich przedsiębiorstw w dobie integracji z Unią Europejską*. Warszawa.
Pietraś M., 2000: *Bezpieczeństwo ekologiczne w Europie. Studium politologiczne*. Lublin.
Pillsbury M., ed., 1998: *Chinese Views of Future Warfare*, Washington, D.C.
Piotrowski M.A., 2012: *Postęp programu nuklearnego Iranu w ocenach Stanów Zjednoczonych, Izraela i Międzynarodowej Agencji Energii Atomowej*. „Sprawy Międzynarodowe", nr 4.
Piotrowski M.A., 2013: *Proliferacja, obrona antybalistyczna i odstraszanie nuklearne na Bliskim Wschodzie. Nowy wyścig zbrojeń czy stabilizacja regionu?*. „Sprawy Międzynarodowe", nr 3.
Podraza A., 2013: *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.
Podraza A., Potakowski P., Wiak K., red., 2013: *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.
Pogońska-Pol M., 2012: *Działalność Organizacji Narodów Zjednoczonych w czasie pierwszej wojny arabsko-izraelskiej 1948—1949*. W: Bania R., Zdulski K., red., *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*. Łódź.
Popiuk-Rysińska I., 1992: *Środki polityki zagranicznej państwa*. W: Kukułka J., red., *Polityka zagraniczna państwa*. Warszawa.
Porębski L., 2001: *Perspektywy wprowadzenia elektronicznej demokracji w działalności uczelni*. W: Haber L.H., red., *Mikrospołeczność informacyjna*. Kraków.
Portnoy M., Goodman S., 2009: *Regional Intergovernemntal Organisations*. In: Portnoy M., Goodman S., eds., *Global Initiatives to Secure Cyberspace. An Emerging Landscape*. New York.
Portnoy M., Goodman S., eds., 2009: *Global Initiatives to Secure Cyberspace. An Emerging Landscape*. New York.
Przybycień K.K., 2007: *Edukacja „ery informacji"*. W: Drzyzga P., red., *Nowe media a tradycyjne środki przekazu*. Kraków.

Przybylska-Maszner B., ed., 2011: *The Arab Spring*. Poznań.
Pudełko M., 2013: *Prawdziwa historia Internetu*. Piekary Śląskie.
Pufeng W., 1998: *The Challenge of Information Warfare*. In: Pillsbury M., ed., *Chinese Views of Future Warfare*. Washington, D.C.
Raas W., Long A., 2007: *Osirak Redux? Assesing Israeli Capabilities to Destroy Iranian Nuclear Facilities*. „International Security". Vol. 31, no. 4.
Record J., 1997: *Congress, Information Technology, and the Use of Force*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Regina-Zacharski J., 2010/2011: *Analityczne definicje wojny*. „Studia Geopolitca", nr 1.
Repko E.M., 2007: *The Israeli — Syrian Conflict: Prospects for a Resolution*. „The Journal of International Policy Solutions". Vol. 7.
Restarting Israeli — Syrian Negotiations. „Crisis Group Middle East Report", no. 63/2007.
Richards J., 2009: *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*. „International Affairs Review". Vol. 18, no. 2.
Rid T., 2012: *Cyber War Will Not Take Place*. „Journal of Strategic Studies", no. 1.
Rid T., 2013: *Cyber War Will Not Take Place*. New York.
Rischard J.-F., 1997: *Connecting Developing Countries to the Information Technology Revolution*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Robinson J., 1997: *Technology, Change, and the Emerging International Order*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.
Rorive I., 2009: *What can be done against cyber hate? Freedom of speech versus hate speech in the Council of Europe*. „Cardozo Journal of International & Comparative Law". Vol. 17, no. 3.
Roscini M., 2010: *World Wide Warfare — Ius ad bellum and the Use of Cyber Force*. In: von Bogdandy A., Wolfrum R., eds., *Max Planck Yearbook of United Nations Law*. Leiden.
Rosenau J.N., 2000: *The Information Revolution: Both Powerful and Neutral*. In: Copeland T.E., ed., *The Information Revolution and National Security*. Carlisle.
Rosenfield D.K., 2009: *Rethinking cyber war*. „Critical Review". Vol. 21, no. 1.
Roszczynialski W., 2003: *E-Learning — narzędzie społeczeństwa informacyjnego*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.
Rothert A., 2004: *Technologia a demokracja*. W: Adamowski J., Jas M., red., *Demokracja a nowe środki komunikacji społecznej*. Warszawa.
Rutkowski P., 2014: *Strategia cyberbezpieczeństwa Unii Europejskiej — pilne wyzwania, nieśpieszna debata*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.
Ruus K., 2008: *Cyber War I: Estonia Attacked from Russia*. „European Affairs", no. 9:1.
Saalbach K.-P., 2013: *Cyber War. Methods and Practice*. Osnabrück.
Saco D., 2002: *Cybering Democracy: Public Space and the Internet*. Minneapolis — London.

Sampson N.R., Hair D., eds., 1990: *Natural Resources of the 21st Century*. Washington, D.C.

Sandvik K.B., 2012: *Cyberwar as an Issue of International Law*. „Prio Policy Brief", no. 04.

Saramak B., 2014: *„Biały wywiad" w służbie terroryzmu*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Schackelford S.J., 2009: *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. „Berkeley Journal of International Law". Vol. 27, no. 1.

Schmitt M.N., ed., 2013: *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge.

Schweitzer Y., Siboni G., Yogev E., 2011: *Cyberspace and Terrorist Organizations*. „Military and Strategic Affairs". Vol. 3, no. 3.

Segal R.L., 1997: *The Coming Electronic Commerce (R)evolution*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Sharma A., 2009: *Cyber Wars: A Paradigm Shift from Means to Ends*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.

Shimeall T., 2001: *Countering cyber war*. „NATO Review". Vol. 49, no. 4.

Sienkiewicz P., 2003: *Wizje i modele wojny informacyjnej*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość?* Kraków.

Sienkiewicz P., Świeboda H., 2006a: *Analiza systemowa zjawiska cyberterroryzmu*. „Zeszyty Naukowe AON". T. 63, nr 2.

Sienkiewicz P., Świeboda H., 2006b: *Niebezpieczna przestrzeń cybernetyczna*. „Transformacje", nr 1—4.

Sienkiewicz P., Świeboda H., 2009: *Sieci teleinformatyczne jako instrument państwa — zjawisko walki informacyjnej*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Silaev N., Pkhaladze T., 2011: *Russian — Georgian Relations and the context of European Security*. In: Gogolashvili K., ed., *Russia and Georgia: Searching the Way Out*. Tbilisi.

Silicki K., 2009: *Unia Europejska a bezpieczeństwo teleinformatyczne — inicjatywy i wyzwania*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Siwicki M., 2013: *Cyberprzestępczość*. Warszawa.

Skrzypczak J., 2011: *Bezpieczeństwo teleinformatyczne w świetle Europejskiej konwencji o cyberprzestępczości*. „Przegląd Strategiczny", nr 1.

Skwarzyński M., 2013: *Prawa człowieka a wprowadzanie stanów nadzwyczajnych z uwagi na działania w cyberprzestrzeni*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.

Šmihula D., 2010: *Waves of technological innovations and the end of the information revolution*. „Journal of Economics and International Finances", no. 2(4).

Smith M.R., Marx L., eds., 1994: *Does Technology Drive History?* Cambridge.

Smith-Bers J., 1997: *Banking and Cyberspace: The New Promised Land*. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair.

Sofaer A.D., Clark D., Diffie W., 2010: *Cyber Security and International Agreements*. In: *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.

Sokała W., 2014: *Współczesna edukacja — tarczą przeciw BMM (Broni Masowej Manipulacji)?* W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Sokolski H.D., ed., 2004: *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*. Carlisle.

Soltanifar M., 2005: *US — Russian Rivalry in the Caucasus: Towards a New Cold War?* „Global Dialogue", no. 3—4.

Stachura J., 2007: *Stany Zjednoczone — supermocarstwo „po przejściach"*. W: Balcerowicz B., Haliżak E., Kuźniar R., Popławski D., Szlajfer H., red., *Rocznik Strategiczny 2006/2007*. Warszawa.

Stefanowicz B., 2013: *Informacja. Wiedza. Mądrość*. Główny Urząd Statystyczny. T. 66. Warszawa.

Stępień T., 2012: *Kultury, przestrzenie i technologie jako transdyscyplinarne elementy nauki o stosunkach międzynarodowych*. „Przegląd Strategiczny", nr 1.

Sterner E., 2012: *The Paradox of Cyber Protest*. „Policy Outlook", George C. Marshall Institute (April).

Suchorzewska A., 2013: *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*. W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.

Sułek M., 2012: *Prakseologiczna teoria stosunków międzynarodowych*. „Przegląd Strategiczny", nr 1.

Sullivan G.R., Coroalles A.M., 1995: *The Army in the Information Age*. Carlisle.

Swanson L., 2010: *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian — Georgian Cyber Conflict*. „Loyola of Los Angeles International and Comparative Law Review". Vol. 32.

Symonides J., 2012: *Spory terytorialne ma Morzu Południowochińskim*. „Stosunki Międzynarodowe — International Relations", nr 2.

Szarfenberg R., 2004: *Polityka społeczna a nowe media*. W: Adamowski J., Jas M., red., *Demokracja a nowe środki komunikacji społecznej*. Warszawa.

Szeptyński P., 2014: *Współczesne wyzwania w zarządzaniu bezpieczeństwem informacji*. W: Liedel K., Piasecka P., Aleksandrowicz T.R., red., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*. Warszawa.

Szpunar M., 2012: *Nowe-stare medium.* Warszawa.

Szubrycht T., 2004: *Sieciocentryczność — mity i rzeczywistość*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 4.

Szubrycht T., 2005: *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1.

Szubrycht T., Szymański T., 2005: *Broń elektromagnetyczna jako nowy środek walki w erze informacyjnej*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 3.

Szymczyk K., 2012: *Irański program nuklearny jako czynnik warunkujący stosunki międzynarodowe w obszarze i poza obszarem MENA*. W: Bania R., Zdulski K., red., *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*. Łódź.

Szyszłak T., 2011: *System ochrony mniejszości narodowych w ramach Wspólnoty Niepodległych Państw*. W: Kapuśniak T., red., *Wspólnota Niepodległych Państw: fragmegracja — bezpieczeństwo — konflikty etniczne*. Lublin.

Tabansky L., 2011: *Basic Concepts in Cyber Warfare*. „Military and Strategic Affairs". Vol. 3, no. 1.

Taddeo M., 2012: *An Analysis for a Just Cyber Warfare*. In: Czosseck C., Ottis R., Ziolkowski K., eds., *4th International Conference on Cyber Conflict*. Tallin.

Tarnogórski R., 2009: *Konwencja o cyberprzestępczości — międzynarodowa odpowiedź na przestępczość ery informacyjnej*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Tchórzewski J., Zając K., Fronczek M., Ostaszewski M., 2003: *Elektroniczne zarządzanie administracją rządową wspomagane systemami sztucznej inteligencji*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Telang R., Wattal S., 2007: *An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price*. „IEEE Transactions on Software Engineering". Vol. 33, no. 8.

Telecommunications and Democracy. In: Alberts D.S., Papp D.S., eds., *The Information Age: An Anthology on Its Impact and Consequences*. Fort McNair 1997.

Terlikowski M., 2009: *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*. W: Madej M., Terlikowski M., red., *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.

Terlikowski M., Rękawek K., Kozłowski A., 2014: *Cyberterrorism: The Threat that Never Was*. „PISM Strategic File", no. 4.

The American Heritage Science Dictionary. Boston 2002.

Thonnard O., Mees W., Dacier M., 2009: *Behavioral Analysis of Zombie Armies*. In: Czosseck C., Geers K., eds., *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam.

Tikk E., 2011a: *Comprehensive legal approach to cyber security*. Tartu.

Tikk E., 2011b: *Ten Rules for Cyber Security*. „Survival". Vol. 53, no. 3.

Toffler A., 1980: *The Third Wave.* New York.

Topolski I., 2013: *Polityka Federacji Rosyjskiej wobec państw Europy Wschodniej*. Lublin.

Touré H.I., 2011a: *Cyberspace and the Threat of Cyberwar*. In: Touré H.I., ed., *The Quest for Cyber Peace*. Geneva.

Touré H.I., 2011b: *The International Response to Cyberwar*. In: Touré H.I., ed., *The Quest for Cyber Peace*. Geneva.

Touré H.I., ed., 2011: *The Quest for Cyber Peace*. Geneva.

Trejderowski T., 2013: *Kradzież tożsamości. Terroryzm informatyczny*. Warszawa.

Van Eeten M.J.G., Bauer J.M., 2008: *Economics of Malware: Security Decisions, Incentives and Externalities*. „STI Working Paper", no. 1.

Van Eeten M.J.G., Bauer J.M., Asghari H., Tabatabaie S., 2010: *The Role of Internet Service Providers in Botnet Mitigation*. „OECD Science, Technology and Industry Working Papers", no. 05.

Vinge V., 2001: *True Names and the Opening of the Cyberspace Frontier*. New York.

Von Bogdandy A., Wolfrum R., eds., 2010: *Max Planck Yearbook of United Nations Law*. Leiden.

Von Clausewitz C., 2010: *O wojnie*. Przeł. A. Cichowicz i L. Koc. Kraków.

Wall D.S., 2007: *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge.

Warden J.A., 1995: *Enemy as a System*. „Airpower Journal", no. 9.

Watts S., 2012: *The Notion of Combatancy in Cyber Warfare*. In: Czosseck C., Ottis R., eds., *2012 4th International Conference on Cyber Conflict*. Tallin.

Weathersby K., 1993: *Soviet Aims in Korea and the Origins of the Korean War, 1945—1950: New Evidence from Russian Archives*. „Florida State University Working Paper", no. 8.

Weimann G., 2005: *Cyberterrorism: The Sum of All Fears?* „Studies in Conflict & Terrorism". Vol. 28, no. 2.

Weldemariam K., Villafiorita A., Mattioli A., 2007: *Assessing Procedural Risks and Threats of e-Voting: Challenges and an Approach*. In: Alkassar A., Volkamer M., eds., *E-voting and Identity*. Bochum.

Westby J.R., 2011: *Conclusion*. In: Touré H.I., ed., *The Quest for Cyber Peace*. Geneva.

Westby J.R., Wegener H., Barletta W., eds., 2010: *Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty*. New York.

Willson D.L., 2012: *Cyberwar or Cyber Cold War*. „ISSA Journal" (September).

Włodowska-Bagan A., 2012: *Badania nad rywalizacją w nauce o stosunkach międzynarodowych*. „Stosunki Międzynarodowe — International Relations", nr 1.

Wojciechowski S., 2009: *Terroryzm. Analiza pojęcia*. „Przegląd Bezpieczeństwa Wewnętrznego", nr 1.

Wolfers A., 1952: „*National Security*" *as an Ambiguous Symbol*. „Political Science Quarterly". Vol. 67, no. 4.

Wortzel L.M., 2014: *The Chinese People's Liberation Army and Information Warfare.* Carlisle.

Woźniak M.G., red., 2011: *Nierówności społeczne a wzrost gospodarczy. Społeczeństwo informacyjne — regionalne aspekty rozwoju*. Rzeszów.

Wu T.S., 1997: *Cyberspace sovereignty? The Internet and the international system*. „Harvard Journal of Law & Technology". Vol. 10, no. 3.

Wytrążek W., 2013: *Wirtualna przestrzeń publiczna — szansa czy zagrożenie dla administracji*? W: Podraza A., Potakowski P., Wiak K., red., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa.

Yagil L., 2002: *Terroristes et Internet. La Cyberguerre.* Montréal.

Zacher L.W., 2003: *Od społeczeństwa informacyjnego do społeczeństwa wiedzy (dylematy tranzycyjne: między informacją, wiedzą i wyobraźnią)*. W: Haber L.H., red., *Społeczeństwo informacyjne — wizja czy rzeczywistość*? Kraków.

Zając J., 2005: *Środki i metody polityki zagranicznej państwa*. W: Zięba R., red., *Wstęp do teorii polityki zagranicznej państwa*. Toruń.

Zając J., 2009: *Konflikt arabsko-izraelski w świetle teorii konfliktów międzynarodowych*. „Stosunki Międzynarodowe — International Relations", nr 1—2.
Zając J., 2011: *Polityka zagraniczna USA*. W: Łoś-Nowak T., red., *Polityka zagraniczna. Aktorzy — potencjały — strategie*. Warszawa.
Zając J., red., 2006: *Polityka zagraniczna USA po zimnej wojnie*. Toruń.
Zakrzewski S., 2013: *Bezpieczeństwo socjalne a wykluczenie społeczne*. „Przegląd Strategiczny", nr 1.
Zawojski P., 2010: *Cyberkultura*. Warszawa.
Zhang L., 2012: *A Chinese perspective on cyber war.* „International Review of the Red Cross". Vol. 94, no. 886.
Zhao S., 2013: *Chinese Foreign Policy as a Rising Power to find its Rightful Place*. „Perception". Vol. XVIII, no. 1.
Zhimin C., Lulu C., 2013: *The Power Strategy of Chinese Foreign Policy. Bringing Theoretical and Comparative Studies Together*. „NFG Working Paper", no. 3.
Zięba R., 1999: *Instytucjonalizacja bezpieczeństwa europejskiego*. Warszawa.
Zięba R., 2005a: *Cele polityki zagranicznej państwa*. W: Zięba R., red., *Wstęp do teorii polityki zagranicznej państwa*. Toruń.
Zięba R., 2005b: *Uwarunkowania polityki zagranicznej państwa*. W: Zięba R., red., *Wstęp do teorii polityki zagranicznej państwa*. Toruń.
Zięba R., red., 2005: *Wstęp do teorii polityki zagranicznej państwa*. Toruń.
Ziolkowski K., 2013: *Confidence Building Measures for Cyberspace — Legal Implications*. Tallin.
Żukrowska K., 2006: *Pojęcie bezpieczeństwa i jego ewolucja*. W: Żukrowska K., Grącik M., red., *Bezpieczeństwo międzynarodowe. Teoria i praktyka*. Warszawa.
Żukrowska K., Grącik M., red., 2006: *Bezpieczeństwo międzynarodowe. Teoria i praktyka*. Warszawa.
Żurawski vel Grajewski P., 2012: *Bezpieczeństwo międzynarodowe. Wymiar militarny*. Warszawa.

Artykuły prasowe

Bohlen C.: *After Shevardnadze's Plea, Russia May Help Georgians*. „The New York Times", 20.10.1993.
Borger J.: *Pentagon kept the lid on cyber war in Kosovo*. „The Guardian", 9.11.1999.
Brągoszewski P.: *Świat żywych trupów*. „PC World", 05.2007.
Bumiller E.: *Panetta Warns of Dire Threat of Cyberattack on U.S.* „The New York Times", 11.10.2012.
Cohen G., Hirschauge O.: *Reports on Internet slowdowns as anti-Israel hackers prepare Sept. 11 attacks*. „Haaretz", 10.09.2013.
Davis J.: *Web War One*. „Wired", 09.2007.
Drucker P.F.: *The Next Information Revolution*. „Forbes", 24.08.1998.

Fitchett J.: *French Report Accuses U.S. of Industrial Sabotage Campaign*. „The New York Times", 19.07.1995.
Gellman B., Poitras L.: *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. „The Washington Post", 6.06.2013.
Gostiew A., 2013: *Rozwój cyberbroni*. „DLP Expert", nr 1(4).
Gottlieb B.: *HacK, CouNterHacK*. „The New York Times", 3.10.1999.
Graham B.: *Hackers Attack Via Chinese Web Sites*. „Washington Post", 28.08.2005.
Gross M.J.: *A Declaration of Cyber War*. „Vanity Fair", 04.2011.
Hauben M.: *Computer Hacking, A Crime?* „ACN". Vol. 2, no. 1/1989.
Kirk D.: *9 North Koreans Dead in Submarine*. „The New York Times", 27.06.1998.
Łapiński A.: *Potomkowie Stuxnetu*. „DLP Expert", nr 1(4)/2013.
Leaflets and e-mail urge Iraqi commanders to surrender. „New Straits Times", 21.03.2003.
Lucky R.W.: *Cyber Armageddon*. „IEEE Spectrum", 09.2010.
Marbach W.D.: *Beware: Hackers at play*. „Newsweek", 5.09.1982.
McFadden R.D.: *The West Condemns the Crackdown*. „The New York Times", 5.06.1989.
Nakashima E., Warrick J.: *Al-Qaeda's Online Forums Go Dark for Extended Period*. „The Washington Post", 2.04.2012.
Thornburgh N.: *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*. „Time", 5.09.2005.
War in the Fifth Domain. „The Economist", 1.07.2010
Zakrzewski A.: *Jak to jest z tym Stuxnetem, Flamem, Duqu?* „DLP Expert", nr 1(4)/2013.
Ziarek M.: *Współczesne cyberbronie*. „DLP Expert", nr 1(4)/2013.

Dokumenty i raporty

2012 Norton Cybercrime Report. Symantec 2012.
A Comprehensive Resolution of the Korean War. „United States Institute of Peace Special Report", no. 106, May 2003.
A New Era of Cyber Warfare with Flame. „CERT-MU e-Security Newsletter". Vol. 2, no. 2/2012.
A strategy for a Secure Information Society — „Dialogue, partnership and empowerement". Communication From the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Commission of the European Communities COM (2006) 251.
Achievements and next steps: towards global cyber-security. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Commission of the European Communities. COM (2011) 163 final. Brussels. 31.03.2011.

Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Government at the NATO Summit in Lisbon. 19—20.11.2010.

Additional protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. „Série de traités européens", no. 189.

Administration Strategy to Mitigate the Theft of U.S. Trade Secrets. Executive Office of the President of the United States. February 2013.

Adoption of the agenda. United Nations Conference on Trade and Development. TD/365. Midrand. 01.04.1996.

Albright D., Brannan P., Walrond C., 2011: *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. „ISIS Report". Institute for Science and International Security. 15.02.2011.

Alperovitch D., 2011: *Revealed: Operation Shady RAT*. „McAfee White Paper". Ver. 1.1. Santa Clara.

An Overview of Inter-Korean Relations. „NCNK Issue Brief". The National Committee on North Korea.

Analysis Report on Flame Worm Samples. Antiy Labs. Version 1.3.0. July 2012.

Anderson R., Barton C., Böhme R., Clayton R., van Eeten M.J.G., Levi M., Moore T., Savage S.,2012: *Measuring the Cost of Cybercrime*. Workshop on the Economics of Information Security. WEIS 2012. Berlin 25—26.06.2012.

Annex A: A Reference Framework for Action on Electronic Commerce. APEC. 1998/ TELMM/JMS/2. Singapore 03—05.06.1998.

Annex A: APEC Telecommunications and Information Working Group (TEL) Program of Action. APEC. 2002/TELMM/JMS/1. Shanghai 30.05.2002.

Annex A: APEC Telecommunications and Information Working Group Program of Action. APEC. 2005/TELMIN/JMS/1. Lima 01.06.2005.

Annex B: Statement on the Security of Information and Communications Infrastructures. APEC. 2002/TELMM/JMS/2. Shanghai 30.05.2002.

Annex C: APEC Principles of Interconnection. APEC. 2000/TELMM/JMS/3. Cancun 24—26.05.2000.

Annex E: APEC Principles for Action against Spam. APEC. 2005/TELMIN/JMS/5. Lima 01—03.06.2005.

Annual Report PandaLabs. Panda Security. 2010.

Annual Report to Congress. Military and Security Developments Involving the People's Republic of China 2013. U.S. Department of Defence. Washington, D.C. 2013.

APEC—OECD Workshop on Security of Information Systems and Networks: Summary. Directorate for Science, Technology and Industry. Organisation for Economic Co-operation and Development. DSTI/ICCP/REG(2005)13. 07.12.2005.

APT1. Exposing One of China's Cyber Espionage Units. Mandiant 2012.

Are the 2011 and 2013 South Korean Cyberattacks Related? „Symantec Security Response". 29.03.2013.

Ashton C., 2012: *Cyber security: an open, free and secure Internet*, European Commission. SPEECH/12/685. Budapest 04.10.2012.

Ashton C., 2012: *Speech by EU High Representative Catherine Ashton on Cyber security: an open, free and secure Internet*. Budapest 04.10.2012. European Union A 440/12.

Assessment of the progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society. ECOSOC Resolution 2012/5.

Astana Declaration of the 10th Anniversary of the Shanghai Cooperation Organisation. Shanghai Cooperation Organisation. Astana 15.06.2011.

Atkinson R.D., McKay A.S., 2007: *Understanding the Economic Benefits of the Information Technology Revolution.* The Information Technology & Innovation Foundation. March.

Auvinen A.-M., 2012: *Social Media — The New Power of Political Influence*. Centre for European Studies. Suomen Toivo Think Tank. Brussels—Helsinki.

Baseline capabilities for national/governmental CERTs. European Network and Information Security Agency. Version 1.0. Initial Draft. December 2009.

Bencsáth B., Pék G., Buttyán L., Félegyházi M., 2011: *Duqu: A Stuxnet-like malware found in the wild*. Technical Report by Laboratory of Cryptography and System Security (CrySys). Budapest University of Technology and Economics. v0.93, 14.10.2011

Bendiek A., 2012: *European Cyber Security Policy*. „SWP Research Paper". October. RP 13.

Biała Księga Bezpieczeństwa Narodowego RP. Biuro Bezpieczeństwa Narodowego. Warszawa 2013.

Billo C.G., Chang W., 2004: *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*. Institute for Security Technology Studies. Hanover.

Boland J., 2011: *Ten Years of the Shanghai Cooperation Organization: A Lost Decade? A Partner for the U.S.?* „21st Century Defense Initiative Policy Paper". 20.06.2011.

Brennan J.W., 2011: *United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling*. „USAWC Civilian Research Project". Carlisle Barracks. 15.03.2012.

Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on April 3 2008. NATO Official Texts 03.04.2008.

Burgess R.L., 2010: *Iran's Military Power*. Statement before the Committee on Armed Services United States Senate. 14.04.2010.

Byres E., Ginter A., Langill J., 2011: *How Stuxnet Spreads — A Study of Infection Paths in Best Practice Systems*. „Tofino Security, Abterra Technologies, ScadaHacker.com White Paper". 22.02.2011.

Canada's Cyber Security Strategy. For a stronger and more prosperous Canada. Her Majesty the Queen in Right of Canada. Canada 2010.

Carr J., Rios B., Plansky D., Walton G., Devost M., Moran N., Givner-Forbes R., Silverstein S., 2009: *Project Grey Goose Phase II Report: The evolving state of cyber warfare*. Greylogic 20.03.2009.

Cartwright J.E., *Joint Terminology for Cyberspace Operations*, Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates, Washington D.C. 2010

Castro D., *Data Privacy Principles for Spurring Innovation*, The Information Technology & Innovation Foundation, June 2010

Castro D., 2009: *Health IT. Explaining International IT Application Leadership*. The Information Technology & Innovation Foundation. September.

Chanlett-Avery E., Rinehart I.E., 2014: *North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation*. „CRS Report Prepared for Members and Committees of Congress". 15.01.2014

Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of North Atlantic Council in Chicago. 20.05.2012

Clarke Z., Clawson J., Cordell M., 2003: *A brief history of hacking*… „Historical Approaches to Digital Media". November.

Coleman K., 2008: *Cyber Warfare Doctrine. Addressing the Most Significant Threat of the 21st Century*. „The Technolytics Institute Analysis". 06.01.2008

Commission decision concerning the security of information systems used by the European Commission. C(2006) 3602. 16.08.2006

Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology. Hearing before the Subcommittee on Oversight and Investigations of the Committee on Foreign Affairs, House of Representatives, One Hundred Twelfth Congress, First Session. Serial No. 112—14.

Comprehensive National Cybersecurity Initiative. The White House. Washington, D.C. 2008.

Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime. February 2013.

Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. Organisation for Economic Co-operation and Development. 2009.

Conley H.A., Gerber T.P., Moore L., David M., 2011: *Russian Soft Power in the 21st Century. An Examination of Russian Compatriot Policy in Estonia*. Center for Strategic & International Studies. August.

Connect Africa Summit. Outcomes Report, Connect Africa Summit. 05.12.2007.

Consideration of Reports Submitted by States Parties under Article 19 of the Convention. United Nations CAT. CAT/C/EST/CO/4. Geneva 5—23.11.2007.

Convention on Cybercrime. CETS, no. 185. Council of Europe.

Cordesman A.H., Cordesman J.G., 2001: *Cyber-threats. Information Warfare and Critical Infrastructure Protection. Defending the U.S. Homeland*. Washington, D.C.

Cordesman A.H., Nerguizian A., Popescu I.C., *Israel and Syria. The Military Balance and Prospects of War*, Westport 2008

Cordesman A.H., 2008: *Syrian Weapons of Mass Destruction. An Overview*. Center for Strategic & International Studies. 02.06.2008.

Cornish P., ed., 2010: *Executive Summary on Cyber Warfare. A Chatham House Report*. London.

Countering and combating spam. Resolution 52. World Telecommunication Standardization Assembly. Johannesburg 2008.

Countering and combating spam. Resolution 52. World Telecommunication Standardization Assembly Dubai 2012.

Creation of computer incident response teams, particularly for developing countries, and cooperation between them. Resolution 69. The World Telecommunication Development Conference. Hyderabad 2010.

Crime prevention and criminal justice in the context of development. Economic and Social Council Resolution 12/1986. 16th Plenary Meeting. 21.05.1986.

Crime Prevention and Criminal Justice. The General Assembly Resolution 44/72. 78th Plenary Meeting. 08.12.1989.

Critical Terminology Foundations. Russia — U.S. Bilateral on Cybersecurity. EastWest Institute. Moscow State University. New York—Moscow. April 2011.

Cyber Detente Between the United States and China. Shaping the Agenda. EastWest Institute. New York 2012.

Cyber Electromagnetic Activities. Field Manual, no. 3—38. US Army. Washington, D.C. 12.02.2014.

Cyber Espionage. The harsh reality of advanced security threats. Deloitte. Center for Security & Privacy Solutions. 2011.

Cyber Security Strategy for Germany. Federal Ministry of the Interior. February 2011.

Cyber security: emerging threats and challenges. 2010 ECOSOC segment briefing. United Nations 16.07.2010.

Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet economy. Organisation for Economic Co-operation and Development 2012.

Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace. European Commission 07.02.2013. JOIN (2013) final.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Commission. JOIN(2013) 1 final. Brussels 07.02.2013.

Cybersecurity. Resolution 50. World Telecommunication Standardization Assembly. Dubai 2012.

Cybersecurity: A global issue demanding a global approach. Department of Economic and Social Affairs. United Nations 12.12.2011.

Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. The White House. Washington, D.C. 2009.

Dajani M., 2011: *Dry Peace: Syria — Israel and the Water of the Golan*. „The Atkin Paper Series". March.

Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. World Summit on the Information Society. WSIS-03/GENEVA/DOC/4-E. Geneva 12.12.2003.

Declaration of the Tenth Meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation. Shanghai Cooperation Organisation. Tashkent 11.06.2010.

Declaration on the Establishment of the Shanghai Cooperation Organization. Shanghai Cooperation Organization 15.06.2001.

Défense et sécurité des systèmes d'information. Stratégie de la France. Agence Nationale de la Sécurité des Systèmes d'Information. Février 2011.

Definitions and terminology related to building confidence and security in the use of information and telecommunication technology. Resolution 181. International Telecommunication Union. Guadalajara 2010.

Deibert R., Rohozinski R., 2010: *Shadows in the Cloud: Investigating Cyber Espionage 2.0*. Information Warfare Monitor. Shadowserver Foundation. 06.04.2010

Deibert R., Rohozinski R., 2009: *Tracking Gh0stNet. Investigating a Cyber Espionage Network.* Information Warfare Monitor. 29.03.2009.

Deklaracja Milenijna Narodów Zjednoczonych. Rezolucja przyjęta na 55. sesji Zgromadzenia Ogólnego Narodów Zjednoczonych. Ośrodek Informacji ONZ. Warszawa 2002.

Denning D.E., 2000: *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services U.S. House of Representatives. Georgetown University. Washington, D.C. 23.05.2000.

Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. Washington D.C. 15.08.2013.

Department of Defense Dictionary of Military and Associated Terms. Joint Chiefs of Staff U.S. Department of Defense. Washington, D.C. 2001.

Department of Defense Strategy for Operating in Cyberspace. U.S. Department of Defense. July 2011.

Deterrence and Defence Posture Review. NATO Press Release (2012) 063. Chicago 20.05.2012.

Development of Policies for Protection of Critical Information Infrastructures, Ministerial Background Report. Organisation for Economic Co-operation and Development. DSTI/ICCP/REG(2007)20/FINAL. 18.12.2007.

Digital Economy 2002. U.S. Department of Commerce. 31—40 (2002).

Documents of the First Committee. A/C.1/54/INF/1. United Nations General Assembly. 30.09.1999.

Dolven B., Kan S.A., Manyin M.E., 2013: *Maritime Territorial Disputes in East Asia: Issues for Congress*. „CRS Report for Congress". 30.01.2013.

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa or Draft African Union Convention on the Confidence and Security in Cyberspace. African Union Commission. Version 01/09/2012.

Duqu. „McAfee Labs Consolidated Threat Report", v.2.2. McAfee Labs. 01.11.2011.

Dushanbe Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation. Shanghai Cooperation Organisation. Dushanbe 28.08.2008.

Dutta S., Lopez-Claros A., Mia I., 2006: *Israel: Factors in the Emergence of an ICT Powerhouse*. The Global Information Technology Report 2005—2006. Leveraging ICT for Development. World Economic Forum.

Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Report prepared by the Secretariat. Havana 27.08—07.09.1990.

Eisenstadt M., Knights M., 2012: *Beyod Worst-Case Analysis. Iran Likely Responses to an Israeli Preventive Strike*. „Policy Notes", no. 11. The Washington Institute for Near East Policy.

Electrical Numerical Integrator and Computer. United States Patent Office. 04.02.1964.

Ellis B.W., 2001: *The International Legal Implications and Limitations of Information Warfare: What are the Options?* USAWC Strategy Research Project. U.S. Army War College.

Encourage the creation of national computer incident response teams, particularly for developing countries. Resolution 58. World Telecommunication Standardization Assembly. Dubai 2012.

Esquibel E.J., Laurenzano M.A., Xiao J., Zuvich T., 2005: *Cyber Criminal Activity: Methods and Motivations*. University of Washington. Washington, D.C.

Estonia vs. Russia. The DDoS War. InfraGard Birmingham. June 2007.

Estonian Life. Estonian Ministry of Foreign Affairs. Tallin 2004.

European Parliament on the forthcoming World Conference on International Telecommunications (WCIT-2012) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations. European Parliament. 20.11.2012. 2012/2881(RSP).

Europejska agenda cyfrowa. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Komisja Europejska. KOM(2010) 245 wersja ostateczna. Bruksela 26.08.2010.

Exposing One of China's Cyber Espionage Units. Mandiant Report. 2012.

Falkowski M., 2004: *Kaukaz Północny: rosyjski węzeł gordyjski*. „Prace Ośrodka Studiów Wschodnich". Grudzień.

Falliere N., O Murchu L., Chien E., *W32.Stuxnet Dossier*. „Symantec Security Response", Version 1.4. February 2011.

Feakin T., *Enter the Cyber Dragon. Understanding Chinese intelligence agencies' cyber capabilities*. „ASTI Special Report". Issue 50. June 2013.

Final Acts World Conference on International Telecommunications. International Telecommunication Union. Dubai 2012.

Finklea K.M., Theohary C.A., 2012: *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. „CRS Report for Congress". 23.05.2012.

Fisher R., 2011: *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*. Hearing before the Subcommittee on Oversight and Investigations of the Committee on Foreign Affairs. House of Representatives. One Hundred Twelfth Session. 15.04.2011.

Fötinger C.S., Ziegler W., [b.r.w.]: *Understanding a hacker's mind — A psychological insight into the hijacking of identities*. „White Paper by the Danube-University Krems".

Gallis P., 2008: *Enlargement Issues at NATO's Bucharest Summit*. „CRS Report for Congress". 12.03.2008.

Gas Pipeline Cyber Intrusion Campaign. „ICS-CERT Monthly Monitor". April 2012.

Gauss: Abnormal Distribution. Kaspersky Lab Global Research and Analysis Team. 09.08.2012.

GCA Strategy. High-Level Experts Group (HLEG). International Telecommunication Union. November 2007.

Geers K., 2008: *Cyberspace and the Changing Nature of Warfare*. Cooperative Cyber Defence Centre of Excellence. Tallin.

Global Cybersecurity Agenda Brochure. International Telecommunication Union. Geneva 2011.

Global Energy Cyberattacks: „Night Dragon". „McAfee White Paper". 10.02.2011.

Good practice guide for CERTs in the area of Industrial Control Systems. Computer Emergency Response Capabilities considerations for ICS. ENISA. October 2013.

Gordon S., 2008: *Cyberterrorism?* „Symantec Security Response".

Greats news for cyber security of the EU: The EP successfully votes through the Network & Information Security (NIS) directive. European Commission — STATEMENT/14/68. 13.03.2014.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security. United Nations General Assembly. A/65/201.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security. United Nations General Assembly. A/68/98.

Gu Q., Liu P., *Denial of Service Attacks*. In: Bidgoli H., ed., *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*. Vol. 3.

Harley D., Lee A., Borghello C., 2009: *Net of the Living Dead: Bots, Botnets and Zombies*. ESET.

Harley D., Lee A., 2009: *The Root of All Evil? Rootkits Revealed*. ESET White Paper.

Healey J., van Bochoven L., 2012: *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. „Atlantic Council Issue Brief". 27.02.2012

Hong Z., 2007: *China-US Oil Rivalry in Africa*. „EAI Background Brief", no. 349. September.

Huasheng Z., Kuchins A.C., 2012: *China and Afghanistan. China's Interests, Stances, and Perspectives*. „A Report of the CSIS Russia and Euroasia Program". Center for Strategic & International Studies. March.

Hui S., *Engaging an Emerging Superpower: Understanding China as a Foreign Policy Actor*. „Asia Programme Paper". ASP2011/05.

ICTs as Enablers of Development. A Microsoft White Paper. December 2004.

Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development. DSTI/ICCP/REG(2003)5/REVI. 02.07.2003.

International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. ECOSOC Resolution 2004/26.

International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. ECOSOC Resolution 2007/20.

International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. ECOSOC Resolution 2009/22.

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. The White House. May 2011.

Internet Security Threat Report 2013. Symantec. Vol. 18.

ITU Regional Cybersecurity Forum for Africa and Arab States held in Tunis, Tunisia. Draft Meeting Report. RFT/2009/01-E. International Telecommunication Union. Tunis 4—5.06.2009.

ITU Toolkit for Cybercrime Legislation. Telecommunication Development Sector. International Telecommunication Union. Draft Rev. February 2010.

ITU's role in child online protection. Resolution 179. International Telecommunication Union. Guadalajara 2010.

ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies. Resolution 174. International Telecommunication Union. Guadalajara 2010.

Joint Communiqué of Meeting of the Council of the Heads of Government (Prime Ministers) of the SCO Member States. Shanghai Cooperation Organisation. Beijing 14.10.2009.

Joint Communiqué of meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation commemorating the 10th anniversary of the SCO. Shanghai Cooperation Organisation. Astana 15.06.2011.

Joint Declaration on SCO/UN Secretariat Cooperation. Shanghai Cooperation Organisation. 05.04.2010.

Joint Operations. Joint Chiefs of Staff. Joint Publication 3-0. 11.08.2011.

Joint Statement on the Inaugural Meeting of the U.S.-Russia Bilateral Presidential Commission Working Group on Threats to and in the Use of Information and Communication Technology (ICT) in the Context of International Security. Office of the Press Secretary. The White House. 22.11.2013.

Joubert V., Petkova G., 2014: *L'intégration des citoyens dans une stratégie nationale de cyberdéfense. Entre opportunités et contraintes stratégiques*. Note de Fondation pour la Recherche Stratégique. 23.01.2014.

Kahl C.H., Dalton M.G., Irvine M., 2013: *Atomic Kingdom. If Iran Builds the Bomb, Will Saudi Arabia Be Next?* Center for a New American Century. February.

Kan S.A., Morrison W.M., 2013: *U.S. — Taiwan Relationship: Overview of Policy Issues*. „CRS Report Prepared for Members and Committees of Congress". 18.11.2013.

Karabeshkin L., 2007: *Russian — Lithuanian Relations: Between Negative Perception Stereotypes and Pragmatic Cooperation*. „Lithuanian Annual Strategic Review 2006". Vilnius.

Kaye D.D., Nader A., Roshan P., 2011: *Israel and Iran. A Dangerous Rivalry*. RAND National Defense Research Institute. Santa Monica.

Kerr P.K., 2009: *Iran's Nuclear Program: Status*. „CRS Report for Congress". 12.11.2009.

Kerr P.K., 2013: *Iran's Nuclear Program: Teheran's Compliance with International Obligations*. „CRS Report Prepared for Members and Committees of Congress". 20.12.2013.

Key indicators for developed and developing countries and the world (totals and penetration rates). International Telecommunications Union. Geneva 27.02.2013.

Kim D., 2013: *Fact Sheet: North Korea's Nuclear and Ballistic Missile Programs*. The Center for Arms Control and Non-Proliferation. July.

Kim S.S., 2007: *North Korean Foreign Relations in the Post-Cold War World*. Strategic Studies Institute. March.

Kirch A., 2001: *Estonian Report on Russian Minority*. Eesti Hariduse ja Teaduse Andmesidevork. Tallin 06.06.2001.

Konwencja Rady Europy o Cyberprzestępczości. Rada Europy. Budapeszt 23.11.2001.

Krekel B., 2009: *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. U.S. — China Economic and Security Review Commission. Northrop Grumman. McLean.

Krepinevich A.W., 2012: *Cyber Warfare. „A Nuclear Option"?*. Center for Strategic and Budgetary Assessments.

Kyrgyzstan Country Profile. „Central Asia Executive Summary Series", no. 2/2009.

Labovitz C., Ahuja A., Jahanian F., 1998: *Experimental Study of Internet Stability and Wide-Area Backbone Failures*. Tech. Rep. CSE-TR-382-98. University of Michigan.

Langner R., 2013: *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Langner Group. November.

Łapczyński M., 2009: *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*. „Komentarz Międzynarodowy Pułaskiego". 03.05.2009.

Laurinavičius Č., 2006: *The Role of History in the Relationship between Lithuania and Russia.* „Lithuanian Annual Strategic Review 2005". Vilnius.

Lesk M., 2007: *The New Front Line. Estonia under Cyberassault*. „Digital Protection". IEEE Computer Society.

Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. United Nations General Assembly A/66/359. 14.09.2011.

Lewis J.A., 2002: *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies. Washington, D.C.

Lewis J.A., 2010: *Cyber War and Competition in the China — U.S. Relationship*. Center for Strategic & International Studies. May.

Lewis J.A., 2006: *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies. January.

Lewis J.A., 2011: *Cybersecurity: Assessing the immediate threat to the United States*. Center for Strategic & International Studies. 25.05.2011.

Lewis J.A., 2006: *The Architecture of Control: Internet Surveillance in China*. Center for Strategic & International Studies. July.

Lewis J.A., 2012: *Thresholds of Cyberwar*. Center for Strategic and International Studies. September.

Lewis J.A., Timlin K., 2011: *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*. „Ideas for Peace and Security".

Lichocki E., 2008: *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*. Centrum Symulacji i Komputerowych Gier Wojennych. Akademia Obrony Narodowej. Warszawa.

Lipson H.F., 2002: *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Networked Systems Survivability Program. Special Report. CMU/SEI-2002-SR-009. November.

Lisbon Summit Declaration. Issued by the Heads of States and Government participating in the meeting of the North Atlantic Council in Lisbon. 20.11.2010.

Lithuania Country Report. European Network and Information Security Agency. Country Reports. May 2011.

Malware infections in the control environment. „ICS-CERT Monitor". October/November/December 2012.

Matrosov A., Rodionov E., Harley D., Malcho J., 2010: *Stuxnet under the Microscope*. ESET Report 2010. Rev. 1.31.

Maurer T., 2011: *Cyber Norm Emergence at the United Nations — an Analysis of the Activities at the UN Regarding Cyber-Security*. Belfer Center for Science and International Affairs. Harvard Kennedy School. September.

Measuring the Information Society. International Telecommunication Union. Geneva 2011.

Measuring the Information Society. International Telecommunication Union. Geneva 2012.

Measuring the Information Society. International Telecommunication Union. Geneva 2013.

Mechanisms of enhancing cooperation on cybersecurity, including countering and combating spam. Resolution 45. The World Telecommunication Development Conference. Hyderabad 2010.

Mele S., 2013: *Cyber-Weapons: Legal and Strategic Aspects*. Instituto Italiano di Studi Strategici.

Melzer N., 2011: *Cyberwarfare and International Law*. „Ideas for Peace and Security". UNIDIR Resources.

Meyers C., Powers S., Faissol D., 2009: *Taxonomies of Cyber Adversaries and Attacks: a Survey of Incidents and Approaches*. Lawrance Livermore National Laboratory. U.S. Department of Energy. April.

Migdalovitz C., 2010: *Israeli-Arab Negotiations: Background, Conflicts and U.S. Policy*. „CRS Report for Congress". 29.01.2010.

Military and Security Developments Involving the People's Republic of China 2013. Annual Report for Congress. Office of the Secretary of Defense. Washington, D.C. 2013.

Miniotaitė G., 2007: *Lithuania's Evolving Security and Defence Policy: Problems and Prospects*. „Lithuanian Annual Strategic Review 2006". Vilnius.

Ministerial Declaration on the Protection of Privacy on Global Networks. Organisation for Economic Co-operation and Development. Annex to C(98)177/FINAL. 07—09.12.1998.

Moćkun S., 2009: *Terroryzm cybernetyczny — zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*. Biuro Bezpieczeństwa Narodowego. Warszawa. Lipiec.

Mulliner C., Miller C., 2009: *Fuzzing the Phone in your Phone*. Black Hat Conference. 25.06.2009.

Multinational Cyber Defence Capability Development — MN CD2. NATO Communications and Information Agency. Brussels 2013.

Mulvenon J.C., 2013: *Chinese Cyber Espionage*. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law. Congressional-Executive Commission on China 25.06.2013.

Myrli S., *NATO and Cyber Defence*. NATO Parliamentary Assembly. 173 DSCFC 09 E BIS.

Nakhleh H.T., 2007: *The 2006 Israeli War on Lebanon: Analysis and Strategic Implications*. „USAWC Strategy Research Project". 23.03.2007.

National Security Concept of Estonia. Adopted by the Riigikogu. 12.05.2010.

Nelson B., Choi R., Iacobucci M., Mitchell M., Gagnon G., 1998: *Cyberterror. Prospects and Implications*. White Paper, Center for the Study of Terrorism and Irregular Warfare. Canada.

Network and Information Security: Proposal for an European Policy Approach. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Commission of the European Communities COM(2001) 298 Final. Brussels 06.06.2001.

Nichol J., *Kyrgyzstan and the Status of the U.S. Manas Airbase: Context and Implications*. „CRS Report for Congress".

Nichol J., 2009: *Russia — Georgia Conflict in August 2008: Context and Implications for U.S. Interests*. „CRS Report for Congress". 03.03.2009.

Nikitin M.B., 2013: *North Korea's Nuclear Weapons: Technical Issues*. „CRS Report for Congress". 12.02.2013.

Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. United Nations. A/CONF 169/4. Cairo 29.04—08.05.1995.

North Korea: The risks of war in the Yellow Sea. „Asia Report", no. 198/2010.

O'Gorman G., McDonald G., 2012: *The Elderwood Project*. „Symantec Security Response".

Overview of cybersecurity. X.1205. Telecommunication Standardization Sector. International Telecommunication Union. 04.2008.

Paget F., *Hacktivism. Cyberspace has become the new medium for political voices*. „McAfee Labs White Paper".

Pandey S.N., 2010: *Hacktivism of Chinese Characteristics and the Google Inc. Cyber Attack Episode*. Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung.

Park J.K., 2013: *China — U.S. Relations in East Asia. Strategic Rivalry and Korea's Choice*. „A Report of the CSIS Korea Chair". Center for Strategic and International Studies. April.

Plan of Action. World Summit on the Information Society. WSIS-03/GENEVA/DOC/5-E. Geneva 12.12.2003.

Polityka Ochrony Cyberprzestrzeni RP. Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego. Marzec 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej. Ministerstwo Administracji i Cyfryzacji. Agencja Bezpieczeństwa Wewnętrznego. Warszawa. Marzec 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej. Ministerstwo Administracji i Cyfryzacji. Agencja Bezpieczeństwa Wewnętrznego. 25.06.2013.

Polska 2030. Wyzwania rozwojowe. Zespół Doradców Strategicznych Prezesa Rady Ministrów RP. Warszawa 2009.

Press Conference by NATO Secretary General Anders Fogh Rasmussen following the NATO Defence Ministers meeting on 4 June 2013. NATO. 04.06.2013.

Promotion of Activities Relating to Combating Cybercrime, Including Technical Assistance and Capacity-building. ECOSOC Draft Resolution 20/7. April 2011.

Prospective Analysis on Trends in Cybercrime from 2011 to 2020. French National Gendarmerie. Lille 2010.

Protecting Europe from large scale cyber-attacks and disruption: enhancing preparedness, security and resilience. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. Commission of the European Communities. COM(2009) 149 final. Brussels 30.03.2009.

Psaki J., 2013: *Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues*. U.S. Department of State. Press Statement. Washington, D.C., 07.06.2013.

Rabinovich I., 2012: *Israel's View of the Syrian Crisis*. „Analysis Paper". The Saban Center for Middle East Policy at Brookings, no. 28.

„*Race to the Bottom". Corporate Complicity in Chinese Internet Censorship*. Human Rights Watch. Vol. 18, nr 8/2006.

Rattray G.J., Healey J., 2011: *Non-State Actors and Cyber Conflict*. In: Lord K.M., Sharp T., eds., *America's Cyber Future. Security and Prosperity in the Information Age*. Vol. 2. Center for a New American Security. June.

Recommendation of the Council concerning Guidelines for Cryptography Policy. Organisation for Economic Co-operation and Development. C(97)/62/FINAL. 27.03.1997.

Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security 2002. OECD Policies for Information Security & Privacy. OECD 2009.

Recommendation of the Council on Protection of Critical Information Infrastructures 2008. OECD Policies for Information Security & Privacy. Organisation for Economic Co-operation and Development 2009.

Reeder F.S., Chenok D., Evans K.S., Lewis J.A., Paller A., 2012: *Updating U.S. Federal Cybersecurity Policy and Guidance*. „A Report of the CSIS Technology and Public Program". October.

Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). Official Journal L 077. EURLEX. 13.03.2004.

Reid D.N., 2007: *Response to May—July 2006 Cyber Intrusion on Department of State Computer Network*. U.S. Department of State. 19.04.2007.

Remarks by EU High Representative Catherine Ashton at press conference on the launch of the EU's Cyber Security Strategy. European Union. A 69/13. Brussels 07.02.2013.

Resolution 1113 (2011). University for Peace Model United Nations (UPMUNC 2011) Security Council Resolution. 05.03.2011.

Resolution 1874 (2009) Strenghtens Arms Embargo, Calls for Inspection of Cargo, Vessels if State Have „Reasonable Grounds" to Believe Contain Prohibited Items. Security Council. 6141 Meeting (PM).

Resolution 53/70 Adopted by the General Assembly. A/Res/53/70. United Nations General Assembly. 01.04.1999.

Resolution 54/49 Adopted by the General Assembly. A/RES/54/49. United Nations General Assembly. 23.12.1999.
Resolution 54/50 Adopted by the General Assembly. A/RES/54/50. United Nations General Assembly. 23.12.1999.
Resolution 54/201 Adopted by the General Assembly. A/RES/54/201. United Nations General Assembly. 25.01.2000.
Resolution 55/63 Adopted by the General Assembly. A/RES/55/63. United Nations General Assembly. 22.01.2001.
Resolution 56/121 Adopted by the General Assembly. A/RES/56/121. United Nations General Assembly. 23.01.2002.
Resolution 57/239 Adopted by the General Assembly. A/RES/57/239. United Nations General Assembly. 31.01.2003.
Resolution 58/199 Adopted by the General Assembly. A/RES/58/199. United Nations General Assembly. 30.01.2004.
Resolution 60/45 Adopted by the General Assembly. A/RES/60/45. United Nations General Assembly. 06.01.2006
Resolution 61/54 Adopted by the General Assembly. A/RES/61/54. United Nations General Assembly. 19.12.2006.
Resolution 62/17 Adopted by the General Assembly. A/RES/62/17. United Nations General Assembly. 08.01.2008.
Resolution 62/182 Adopted by the General Assembly. A/RES/62/182. United Nations General Assembly. 31.01.2008
Resolution 63/37 Adopted by the General Assembly, A/RES/63/37, United Nations General Assembly, 09.01.2009
Resolution 64/25 Adopted by the General Assembly. A/RES/64/25. United Nations General Assembly. 14.01.2010.
Resolution 64/211 Adopted by the General Assembly. A/RES/64/211. United Nations General Assembly. 17.03.2010.
Resolution 66/24 Adopted by the General Assembly. A/RES/66/24. United Nations General Assembly. 13.12.2011.
Resolution 68/243 Adopted by the General Assembly. A/RES/68/243. United Nations General Assembly. 09.01.2014.
Resolution Amending the Seimas of the Republic of Lithuania Resolution on the Approval of the National Security Strategy. Seimas of the Republic of Lithuania, no. XI-2131. 26.06.2012.
Robinson A., 2012: *Why Cyberterrorism is a Problem in the United States?* „Cyberterrorism Research Paper". 23.05.2012.
Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundation. EastWest Institute. Information Security Institute of Moscow State University. New York—Moscow 2011.
Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011—2016. Ministerstwo Spraw Wewnętrznych i Administracji RP. Czerwiec 2010.
Saint Petersburg Declaration. Building Confidence and Security in the Use of ICT to Promote Economic Growth and Prosperity. APEC. 2012/TELMIN/JMS. Saint Petersburg 07.08.2012.

Saleem M., Hassan J., 2009: *„Cyber warfare", the truth in a real case.* Project Report for Information Security Course. Sweden.

Salem P., 2008: *Syrian — Israeli Peace: A Possible Key to Regional Change*. „Foreign Policy for the Next President". Carnegie Endowment for International Peace. December.

Schreier F., 2015: *On Cyberwarfare*. „DCAF Horizon 2015 Working Paper". Vol. 7.

Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center. Office of the Press Secretary. Department of Homeland Security. Washington, D.C., 30.10.2009.

Security Council Condemns Use of Ballistic Missile Technology in Launch by Democratic People's Republic of Korea. In Resolution 2087 (2013). Security Council 6904th Meeting. SC/10891.

Security Threat Report 2013. Sophos. Boston 2013.

Seongho S., 2007: *Inter-Korean Relations without the U.S. — ROK Alliance*. „NBR/KFiS U.S. — ROK Alliance Conference Paper". Seul.

Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offender. Report prepared by the Secretariat. Milan 26.08—06.09.1985.

Shafie S.J., 2007: *APEC TEL. Regional Workshop on Frameworks for Cyber Security and Critical Information Infrastructure Protection*. Asia-Pacific Economic Cooperation. International Telecommunication Union. Hanoi.

Sharikov P., 2013: *Cybersecurity in Russian — U.S. Relations*. „CISSM Policy Brief". April.

Sherstobitoff R., Liba I., Walter J., *Dissecting Operation Troy: Cyberespionage in South Korea*. „McAfee Labs White Paper".

Shetty S., Kearns I., Lunn S., 2012: *The Baltic States, NATO and Non-Strategic Nuclear Weapons in Europe*. Royal United Services Institute. December.

Siboni G., Kronenfeld S., *Iran's Cyber Warfare*, „INSS Insight", no. 375, 15.10.2012.

Simmons C., Ellis C., Shiva S., Dasgupta D., Wu Q., 2009: *AVOIDIT: A Cyber Attack Taxonomy*. „Technical Report". CS-09-003. Memphis.

Simon S., 2009: *An Israeli Strike on Iran*. „Contingency Planning Memorandum", no. 5. Council on Foreign Relations.

sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. „Technical Report by Laboratory of Cryptography and System Security". Budapest University of Technology and Economics. V1.05. 31.05.2012.

Smith D.J., 2012: *Russian Cyber Operations*. Potomac Institute for Policy Studies.

South Korean Malware Attack. United States Computer Emergency Readiness Team. U.S. Department of Homeland Security. 2013.

Squassoni S., 2006: *Iran's Nuclear Program: Recent Developments*. „CRS Report for Congress". 06.09.2006.

Stanley N., 2010: *The Ongoing Security Paradox*. Bloor Research. London.

Statistical Report on Internet Development in China. China Internet Network Information Center. July 2013.

Storch T., 2012: *Cyberbezpieczeństwo — fundament bezpiecznego społeczeństwa w dobie Internetu*. „TwC Next". Microsoft. 09.03.2012.

Strasbourg/Kehl Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg/Kehl. 04.04.2009.

Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020. Ministerstwo Nauki i Informatyzacji. 24.06.2005.

Strategic War…In Cyberspace. „RAND Research Brief". January 1996.

Strategy for the period 2008—2011 for the United Nations Office on Drugs and Crime. ECOSOC Resolution 2007/12. 25.07.2007.

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. Resolution 130. International Telecommunication Union. Antalya 2006.

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. Resolution 130. International Telecommunication Union. Guadalajara 2010.

Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies. Resolution 149. International Telecommunication Union. Antalya 2006.

Stuxnet Part I: analysis, myths and realities. „ACTUSÉCU", no. 27. February 2011.

Summit Declaration on Defence Capabilities: Toward NATO Forces 2020. NATO Press Release (2012) 064. Chicago 20.05.2012.

Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. Communication from the Commission to the Council and the European Parliament, European Commission. COM(2012) 140 final. Brussels 28.03.2012.

Tafoya W.L., 2011: *Cyber Terror*. „FBI Law Enforcement Bulletin". November.

T-CY Rules of Procedure. Cybercrime Convention Committee. Council of Europe. Strasbourg 21.12.2013.

Ten Days of Rain. Expert analysis of distributed denial-of-service attacks targeting South Korea. „McAfee White Paper". 2011.

The Cyber Index. International Security Trends and Realities. New York, Geneva 2013.

The Eight APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN8). APEC. 2010/TELMIN/JMS. Okinawa 30—31.10.2010.

The Fifth APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN5). APEC. 2002/TELMM/JMS. Shanghai 29—30.05.2002.

The Kyrgyzstan DDoS Attacks of January, 2009: Assessment and Analysis. „Information Warfare Monitor". 28.01.2009.

The National Military Strategy for Cyberspace Operations. Joint Chiefs of Staff. U.S. Department of Defense. Washington, D.C. 2006.

The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development. DSTI/ICCP/REG(2005)1/FINAL. 16.12.2005.

The Seventh APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN7). APEC. 2008/TELMIN/JMS. Bangkok 23—25.04.2008.

The Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN6). APEC. 2005/TELMIN/JMS. Lima 01—03.06.2005.

The Third APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN3). APEC. 1998/TELMM/JMS. Singapore 03—05.06.1998.

The United Nations Global Counter-Terrorism Strategy. Resolution 60/288 Adopted by the General Assembly. A/RES/60/288. United Nations General Assembly. 20.09.2006.

The Use of Internet for Terrorist Purposes. United Nations Office on Drugs and Crime. New York 2012.

Tikk E., Kaska K., Rünnimeri K., Kert M., Tailhärm A.-M., Vihul L., 2008: *Cyber Attacks Against Georgia: Legal Lessons Identified*. Cooperative Cyber Defence Centre of Excellence. Tallin.

Towards a general policy on the fight against cyber crime. Communication From the Commission to the European Parliament, the Council and the Committee of the Regions. Commission of the European Communities. COM(2007) 267 final. Brussels 22.05.2007.

Traktat o funkcjonowaniu Unii Europejskiej — tekst skonsolidowany uwzględniający zmiany wprowadzone przez Traktat z Lizbony, Dz.U.2004.90.864/2

Traktat północnoatlantycki. Dz.U.00.87.970. Waszyngton 04.04.1949.

Treschel A.H., 2007: *Internet Voting in the March 2007 Parliamentary Elections in Estonia*. Report for the Council of Europe, European University Institute. Robert Schuman Centre for Advanced Studies. 31.07.2007.

Tunis Agenda for the Information Society. World Summit on the Information Society. WSIS-05/DOC/6(Rev. 1)-E. Tunis 18.11.2005.

Understanding Cybercrime: A Guide for Developing Countries. Telecommunication Development Sector. International Telecommunication Union. Draft. April 2009.

Understanding Cybercrime: Phenomena, Challanges and Legal Response. Telecommunication Development Sector. International Telecommunication Union. September 2012.

Understanding Cybercrime: Phenomena, Challenges and Legal Response. Telecommunications Development Sector. International Telecommunication Union. September 2012.

United States — Israel Enhanced Security Cooperation Act of 2012. House of Representatives. United States 2012.

Ustawa o zarządzaniu kryzysowym. 26.04.2007. Dz.U. z 2007 r., nr 89, poz. 590.

Ustawa z dnia 16 lipca 2004 r., Prawo telekomunikacyjne. Dz.U., nr 171, poz. 1800, z późniejszymi zmianami.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. z 2005 r., nr 64, poz. 565; Dz.U. z 2006 r., nr 12, poz. 65, nr 73, poz. 501; z 2008 r., nr 127, poz. 817; z 2009 r., nr 157, poz. 1241. Dz.U. z 2010 r., nr 40, poz. 230, nr 167, poz. 1131, nr 182, poz. 1228; Dz.U. z 2011 r., nr 112, poz. 654, nr 185, poz. 1092, nr 204, poz. 1195; Dz.U. z 2012 r., poz. 1407.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002, nr 144, poz. 1204.

Van der Dennen J.M.G., 1980: *On War: Concepts, Definitions, Research Data — a Short Literature Review and Bibliography*. „UNESCO Yearbook on Peace and Conflict Studies 1980".

Virtual Criminology Report 2009. Virtually here: The Age of Cyber Warfare. McAfee Inc. Santa Clara 2009.

Virtual Criminology Report. McAfee. Labs 2009.

W32.Duqu. The precursor to the next Stuxnet. „Symantec Security Response". Version 1.4. 23.11.2011.

Weighing Benefits and Costs of Military Action against Iran, Iran Project. New York 2012.

Wilson C., 2008: *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. „CRS Report for Congress". 29.01.2008.

Wilson C., 2003: *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. „CRS Report for Congress". 17.10.2003.

Wilson Z., 2001: *Hacking: The Basics*. SANS Institute.

Wingfield T.C., 2000: *The Law of Information Conflict: National Security Law in Cyberspace*. Aegis Research Corp.

Wortzel L.M., 2013: *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*. Testimony before the House of Representatives. Committee on Energy and Commerce Subcommittee on Oversight and Investigations House of Representatives. 09.07.2013.

Xu T., 2011: *China and the United States: Hacking Away at Cyber Warfare*. „Asia Pacific Bulletin", nr 135. 01.11.2011.

Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation. Shanghai Cooperation Organisation. Yekaterinburg 16.06.2009.

Zanotti J., 2013: *Israel: Background and U.S. Relations*. „CRS Report for Congress". 01.11.2013.

Zanotti J., Katzman K., Gertler J., Hildreth S.A., 2012: *Israel: Possible Military Strike Against Iran's Nuclear Facilities*. „CRS Report for Congress". 28.09.2012.

Ziomka Z., 2008: *Przyczyny zachowań przestępczych oraz zjawisk patologicznych w świetle teorii socjologicznych*. Szkoła Policji w Katowicach. Katowice.

Zuckerman E., Roberts H., McGrady R., York J., Palfrey J., 2010: *Distributed Denial of Service Attacks against Independent Media and Human Rights Sites*. The Berkman Center for Internet & Society. Harvard University. December.

Źródła internetowe

http://about-threats.trendmicro.com
http://afp.google.com
http://ai.ia.agh.edu.pl
http://archive.newsmax.com
http://archive.org
http://armscontrolcenter.org
http://arstechnica.com
http://bits.blogs.nytimes.com

http://bitsavers.informatik.uni-stuttgart.de
http://blog.economie-numerique.net
http://blogs.mcafee.com
http://blogs.technet.com
http://carnegieendowment.org
http://cert.europa.eu
http://content.time.com
http://conventions.coe.int
http://cpsr.org
http://cs.brown.edu
http://cse.iitkgp.ac.in
http://csis.org
http://cyberaide.googlecode.com
http://cybersecuritymonth.eu
http://ddanchev.blogspot.com
http://defensetech.org
http://definitions.uslegal.com
http://ec.europa.eu
http://edition.cnn.com
http://en.irangreenvoice.com
http://en.ria.ru
http://eng.cnews.ru
http://english.pravda.ru
http://english.yonhapnews.co.kr
http://eprints.eemcs.utwente.nl
http://estonia.eu
http://ezinearticles.com
http://fcw.com
http://flosshub.org
http://ftp.arl.mil
http://giswatch.org
http://gizmodo.com
http://googleblog.blogspot.com
http://icawww1.epfl.ch
http://in.rbth.com
http://irps.ucsd.edu
http://its.dal.ca
http://jmarke.wordpress.com
http://journal.neilgaiman.com
http://kavkazcenter.com
http://knowyourmeme.com
http://konflikty.wp.pl
http://lcweb2.loc.gov
http://library.uniteddiversity.coop
http://listosaur.com
http://mashable.com
http://mathaba.net
http://medialternatives.blogetery.com
http://meeting.afrinic.net
http://money.cnn.com
http://motherboard.vice.com
http://nakedsecurity.sophos.com
http://natemat.pl
http://nationalinterest.org
http://news.bbc.co.uk
http://news.cnet.com
http://news.err.ee
http://news.sky.com
http://niebezpiecznik.pl
http://north-korea.narod.ru
http://nowetechnologie.umk.pl
http://nuclearfiles.org
http://online.wsj.com
http://pclab.pl
http://pespmc1.vub.ac.be
http://rbnexploit.blogspot.com
http://readwrite.com
http://resources.infosecinstitute.com
http://rokdrop.com
http://rt.com
http://science.energy.gov
http://searchsecurity.techtarget.com
http://securityaffairs.co
http://spectrum.ieee.org
http://steinhardt.nyu.edu
http://strategicoutlook.org
http://swampland.time.com
http://technologie.gazeta.pl
http://techpresident.com
http://theaviationist.com
http://thebulletin.org
http://thelede.blogs.nytimes.com
http://theriskyshift.com
http://tremblinguterus.blogspot.com
http://uk.reuters.com
http://umcs.maine.edu
http://usatoday30.usatoday.com
http://visibleearth.nasa.gov
http://vixra.org
http://voiceofrussia.com

http://voices.washingtonpost.com
http://voices.yahoo.com
http://web.archive.org
http://weis2012.econinfosec.org
http://wiadomosci.gazeta.pl
http://wiadomosci.wp.pl
http://world.time.com
http://worldnews.nbcnews.com
http://www.15min.lt
http://www.afcea.org
http://www.airforce-technology.com
http://www.alaskadispatch.com
http://www.aljazeera.com
http://www.allvoices.com
http://www.altair.com.pl
http://www.apec.org
http://www.arbornetworks.com
http://www.arcyber.army.mil
http://www.aribo.eu
http://www.armscontrol.org
http://www.asc-cybernetics.org
http://www.asianewsnet.net
http://www.availabilitydigest.com
http://www.baltic-course.com
http://www.baltictimes.com
http://www.bbc.co.uk
http://www.bizeul.org
http://www.bloomberg.com
http://www.blueridge.com
http://www.brighthub.com
http://www.brookings.edu
http://www.bu.edu
http://www.businessweek.com
http://www.caida.org
http://www.carlisle.army.mil
http://www.cbronline.com
http://www.cbsnews.com
http://www.cc.gatech.edu
http://www.ccdcoe.org
http://www.cert.hu
http://www.cert.org
http://www.certcc.ir
http://www.cfr.org
http://www.chinausfocus.com
http://www.cija.ca
http://www.civil.ge
http://www.cnbc.com
http://www.cnet.com
http://www.coe.int
http://www.commsday.com
http://www.computer.org
http://www.computerweekly.com
http://www.computerworld.com
http://www.crime-research.org
http://www.criticalthreats.org
http://www.cs.arizona.edu
http://www.csi.ucd.ie
http://www.csmonitor.com
http://www.ctc.usma.edu
http://www.cultdeadcow.com
http://www.culturaldiplomacy.org
http://www.cxotoday.com
http://www.cybercrimelaw.net
http://www.cyberwarnews.info
http://www.czn.uj.edu.pl
http://www.dailymail.co.uk
http://www.dallasnews.com
http://www.dbc.wroc.pl
http://www.defence24.pl
http://www.defense.gov
http://www.defensenews.com
http://www.delta.edu
http://www.dhs.gov
http://www.economist.com
http://www.edn.com
http://www.eeca-ict.eu
http://www.eng.nia.or.kr
http://www.eolss.net
http://www.eppgroup.eu
http://www.euractiv.com
http://www.eurasianet.org
http://www.fas.org
http://www.flagtelecom.com
http://www.forbes.com
http://www.forbes.pl
http://www.foreignpolicy.com
http://www.foreignpolicyjournal.com
http://www.foxnews.com
http://www.freerepublic.com
http://www.f-secure.com

http://www.gartner.com
http://www.geopolitika.lt
http://www.go-gulf.com
http://www.google.com
http://www.governmentsecurity.org
http://www.guardian.co.uk
http://www.haaretz.com
http://www.heise-online.pl
http://www.highbeam.com
http://www.hindustantimes.com
http://www.homelandsecuritynewswire.com
http://www.hostexploit.com
http://www.hrichina.org
http://www.huffingtonpost.com
http://www.ieeeghn.org
http://www.impact-alliance.org
http://www.independent.co.uk
http://www.informationweek.com
http://www.infosecurity-magazine.com
http://www.insidegnss.com
http://www.internetgovernance.org
http://www.internetsociety.org
http://www.internetworldstats.com
http://www.interpol.int
http://www.ipcs.org
http://www.iranpolitik.com
http://www.isn.ethz.ch
http://www.israelhayom.com
http://www.israelnationalnews.com
http://www.itp.net
http://www.itu.int
http://www.itworld.com
http://www.jakubduba.pl
http://www.jpost.com
http://www.kaspersky.com
http://www.khaleejtimes.com
http://www.komputerswiat.pl
http://www.koreatimes.co.kr
http://www.lithuaniatribune.com
http://www.livescience.com
http://www.livinginternet.com
http://www.local-life.com
http://www.marinecorpstimes.com
http://www.math.uni.opole.pl
http://www.mhhe.com
http://www.microsoft.com
http://www.mid.ru
http://www.mobilestatistics.com
http://www.mwti.net
http://www.nask.pl
http://www.nationsonline.org
http://www.nato.int
http://www.networksecurity.com
http://www.networkworld.com
http://www.newsday.com
http://www.newyorker.com
http://www.nkeconwatch.com
http://www.nti.org
http://www.nuclear.pl
http://www.nydailynews.com
http://www.nytimes.com
http://www.oecd.org
http://www.out-law.com
http://www.owasp.org
http://www.pagasa.net
http://www.pangaro.com
http://www.pbs.org
http://www.pcadvisor.co.uk
http://www.pcmag.com
http://www.pcworld.com
http://www.pcworld.pl
http://www.pem.cam.ac.uk
http://www.penetrationtest.com
http://www.perihel.at
http://www.personal.utulsa.edu
http://www.pho.pl
http://www.phrack.com
http://www.pl.ism.uw.edu.pl
http://www.protectinternetfreedom.net
http://www.psz.pl
http://www.quotationspage.com
http://www.rawstory.com
http://www.reuters.com
http://www.rfa.org
http://www.rferl.org
http://www.root-servers.org
http://www.sadc.int
http://www.saferinternet.pl
http://www.schneier.com
http://www.scidev.net

http://www.scmp.com
http://www.seculert.com
http://www.securelist.com
http://www.secureworks.com
http://www.spiegel.de
http://www.sptimes.com
http://www.staff.amu.edu.pl
http://www.st-andrews.ac.uk
http://www.stat.ee
http://www.stlr.org
http://www.stm.unipi.it
http://www.stosunki.pl
http://www.strategypage.com
http://www.strato-analyse.org
http://www.submarinecablemap.com
http://www.symantec.com
http://www.tech-faq.com
http://www.technewsdaily.com
http://www.technologytell.com
http://www.techsty.art.pl
http://www.techterms.com
http://www.telegraph.co.uk
http://www.terena.org
http://www.textfiles.com
http://www.thedailybeast.com
http://www.thefreedictionary.com
http://www.theguardian.com
http://www.theinquirer.net
http://www.thenetworkadministrator.com
http://www.theregister.co.uk
http://www.tnode.com
http://www.top500.org
http://www.tripwire.com
http://www.truelithuania.com
http://www.tvn24.pl
http://www.ui.se
http://www.uknof.com
http://www.un.org
http://www.unic.un.org.pl
http://www.unicri.it
http://www.unidir.org
http://www.usatoday.com
http://www.usnews.com
http://www.vice.com
http://www.vm.ee
http://www.washingtonpost.com
http://www.washingtontimes.com
http://www.whitehouse.gov
http://www.wilderssecurity.com
http://www.wired.com
http://www.worldaffairsjournal.org
http://www.worldpoliticsreview.com
http://www.worldsecuritynetwork.com
http://www.wprost.pl
http://www.ynetnews.com
http://www.zdnet.com
https://csis.org
https://history.state.gov
https://kc.mcafee.com
https://mocana.com
https://twitter.com
https://www.cia.gov
https://www.cs.columbia.edu
https://www.damballa.com
https://www.europol.europa.eu
https://www.facebook.com
https://www.ibls.com
https://www.nsm.stat.no
https://www.ria.ee
https://www.shadowserver.org
https://za.news.yahoo.com

Indeks osobowy

Miron Lakomy

Cyberspace as a new dimension of competition and cooperation between countries

Summary

The computer revolution which started in the second half of the 20th century has significantly changed the world in almost every possible aspect and dimension within only a few decades. As it was predicted by some technological determinists, the processes of computerization and IT technologies' implementation have quickly included the consecutive areas of life of individuals and their communities, starting from economy, through science and entertainment, to politics and military service. In terms of the most conspicuous features, such as the overcoming of the previous limitations in processing, sending and storing information, it has brought enormous benefits to humanity. The development of a new unique domain that the cyberspace represents, has become their symbol. Owing to its specific features, for decades it has been determining the functioning of countries and communities to an ever growing extent, permeating the state administration, critical infrastructure, business sector and, finally, armed forces. Their growing dependence on ICT, however, has simultaneously become the reason for the emergence of certain negative tendencies, the cost of which is paid around the world. The universality and global character of information and communication technologies has led to some breakthroughs in the broadly understood safety dimension. Computers and their networks, contributing to the revolution in military affairs (RMA), have at the same time become the source and the platform for the destructive phenomena which, with time, started to be perceived through the prism of a threat to the national and international security. Various individuals, starting with average amateurs, hackers, through hacktivists, cyber-terrorists, and ending with criminal organizations, have gained a prospective possibility to reach even the most vital spheres of the particular countries' security systems owing to cyberspace. In other words, cyberspace has paradoxically become another safety dimension, the role of which has been increasing in proportion to the advances in the processes of computerization and IT technologies' implementation. Still in the 90s of the 20th century, even the most serious computer attacks were usually regarded as, at most, certain nuisance for the central administration, whereas already two decades later, their range has

become large enough to be seen as one of the most serious challenges to the stability of the whole international system.

In this new environment which cyberspace constitutes, these countries which until recently have not evinced any broader interest in the development of skills allowing them to become active in that field, remain the most unique subjects. It started to change at the turn of the 20th and 21st century, when the potential benefits that may be brought by cyberspace became recognized by the political elites of several countries, such as the United States, Russia, China or Israel. On the one hand, the works on the development of the professional and technological potential have been initiated, which allowed for the creating of a more effective security system against computer web breakings. On the other hand, it has been acknowledged that the offensive activeness in teleinformatic sphere may become a convenient weapon in the competition and confrontation with other subjects within the international environment. The objective characteristics of this domain, such as: easily accessed anonymity, "a-geographicity" and "a-territoriality" or low costs of "entry," favoured it. Moreover, the ambiguities connected with interpretation of the binding regulations of international law and mechanisms of political and military cooperation confirmed usefulness of these tools. In only a few years the forerunners have developed very advanced skills in that field, which, in theory, could serve the realization of particular aims in selected specializations.

In this context, the presented study is an attempt to discuss the efficiency of teleinformatic means as the instruments of foreign policy of countries during the post-Cold War period. Taking into account aspects of both competition and cooperation of governments in cyberspace, in the conducted analysis the elements of the theory of foreign policy have been used. The dissertation contains primarily a discussion on the essence and the particular stages of digital revolution which has led to the development of teleinformatic space. Then, its most important features have been characterized from both technical and politological perspectives. On this basis, an attempt to create a simplified typology of teleinformatic dangers to the countries' security has been undertaken, including such phenomena as hacking, hacktivism or cyber-terrorism. Finally, an analysis of the most significant examples of competition and cooperation of countries in cyberspace has been conducted. On the one hand, the following events have been discussed: the situation in Estonia in April and May 2007, in Georgia in August 2008 and in Iran since 2010 (Stuxnet). On the other hand, the instances of cooperation between countries in that field were characterized on the basis of the following examples: The United Nations, The European Union, NATO and The African Union.

Miron Lakomy

Cyberespace en tant que nouvelle dimension de la rivalisation et coopération des États

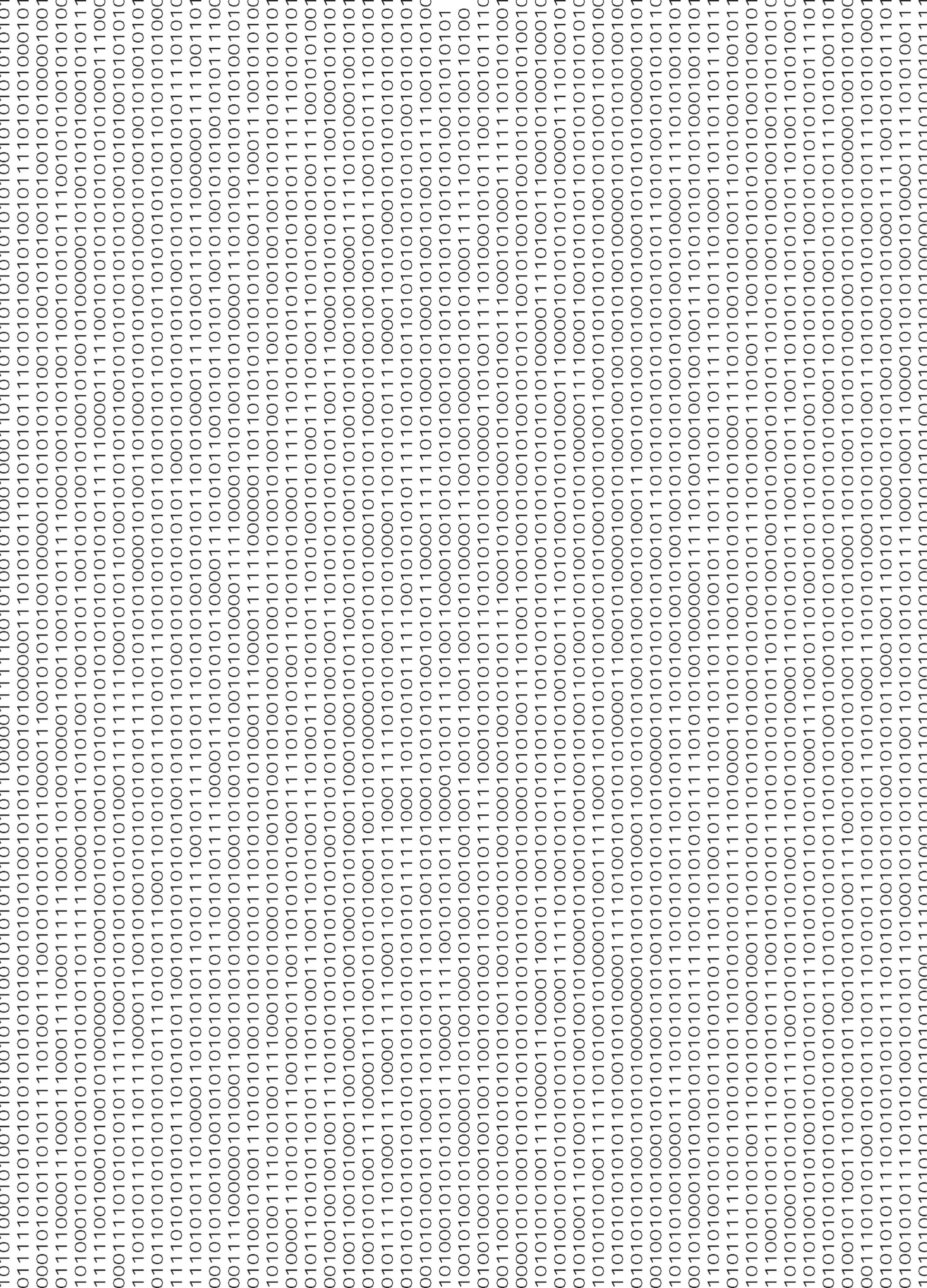
Résumé

La révolution informatique qui s'est déclenchée pour de bon dans la seconde moitié du XX^{e} siècle, à peine en quelques décennies a considérablement changé la physionomie du monde sur presque tous les plans possibles. Conformément aux prévisions d'une partie de déterministes technologiques, les procédés de l'application des ordinateurs au traitement des données et des informations ont vite envahi de nouveaux domaines de la vie des individus et de leur collectivité : de l'économie, en passant par l'enseignement, le divertissement, et allant jusqu'à la politique et l'armée. Étant donné ses traits les plus significatifs consistant à surmonter toutes sortes de limitations liées au traitement, tranfert et stockage d'informations, il a énormément servi à l'humanité. La naissance du cyberespace, nouveau domaine unique dans sa forme, en est devenue le symbole. Ses traits particuliers font que depuis des décennies, il détermine au point de plus en plus haut le fonctionnement des États et des sociétés tout en s'infiltrant dans l'administration des pays, l'infrastructure critique, le secteur du commerce ou encore dans les forces militaires. Leur dépendance croissante de TIC est devenue en même temps la cause de l'apparition de certaines tendances négatives dont on subit les conséquences dans le monde entier. L'universalité et le caractère global des technologies téléinformatiques ont suscité des changements capitaux dans le milieu de sécurité. En contribuant à la révolution dans les affaires militaires (RMA), les ordinateurs et leurs réseaux sont devenus parallèlement la source et la plateforme des phénomènes nuisibles qui, avec le temps, ont commencé à être perçus à travers le prisme des menaces pour la sécurité nationale et internationale. Différents sujets comme simples amateurs, hackers, hactivistes, cyberterroristes ou encore organisations criminelles, justement grâce au cyberespace, ont trouvé une possibilité potentielle de pénétrer même dans les éléments les plus actifs des systèmes nationaux de sécurité. Autrement dit, il est paradoxalement devenu une nouvelle dimension de sécurité dont le rôle augmente proportionnellement aux progrès des procédés liés justement à l'application des ordinateurs au traitement des données et des informations. Encore dans les années 1990, même les plus dangereuses attaques informatiques étaient le plus souvent traitées, au plus, comme un certain incon-

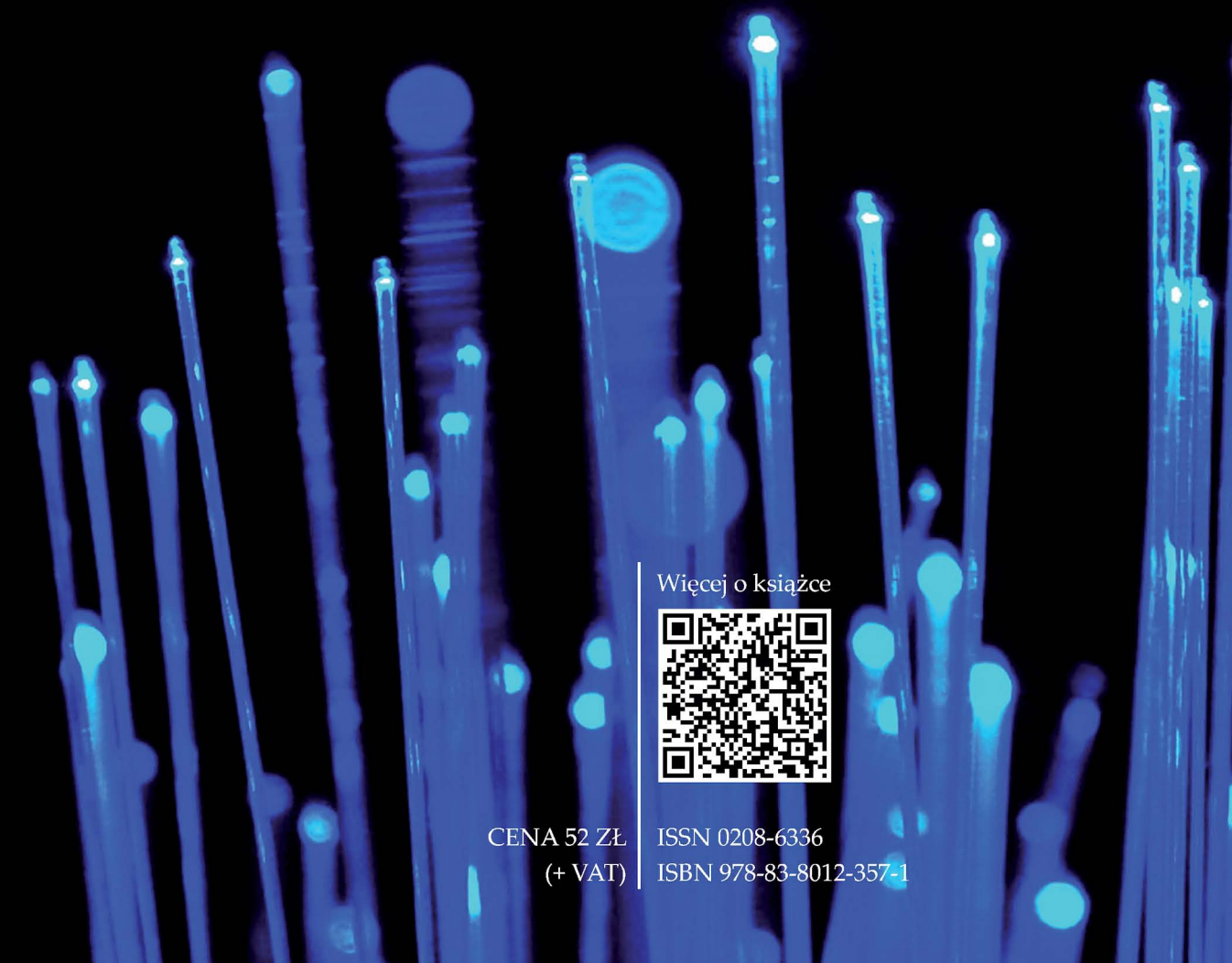
vénient pour l'administration centrale. Cependant, déjà deux décennies plus tard, leur ampleur est devenue si grande que l'on a commencé a y voir l'un des plus importants défis pour la stabilité de tout le système international.

Dans ce nouveau milieu qu'est le cyberespace, un sujet exceptionnel restent les pays qui, il n'y a pas très lontemps, ne portaient pas de grand intérêt à développer leurs propres capacités d'agir dans cette sphère. Cela a commencé à changer plus ou moins à la charnière des XX^{e} et XXI^{e} siècles où les bénéfices potentiels qui en résultaient ont été aperçus par les élites politiques à peine de quelques pays tels que les États-Unis, la Russie, la Chine ou Israël. D'une part, on a commencé à s'occuper au développement du potentiel technologique et celui d'experts ce qui a permis de se protéger plus efficacement contre les effractions informatiques. D'autre part, on a compris qu'une activité offensive dans l'espace téléinformatique pouvait devenir une arme favorable de la rivalisation et confrontation avec d'autres sujets dans le milieu international. Les qualités objectives de ce domaine comme anonymat facilement accessible, « agéographicité » et « aterritorialité » ou bien frais « d'accès » peu élevés le favorisaient encore. De surcroît, les ambiguïtés liées à l'interprétation des dispositions en vigueur du droit international et celle des mécanismes de la coopération politique et militaire ont dénoté l'utilité de ces instruments. En l'occurrence, les procurseurs ont réussi, en quelques années seulement, à créer des capacités avancées dans ce domaine qui ont pu théoriquement servir à réaliser des buts déterminés sur différents plans.

Dans ce contexte, la présente dissertation essaye d'examiner l'efficacité des moyens téléinformatiques comme instruments de la politique extérieure des États dans l'après-guerre froide. Au cours de l'analyse, tout en prenant en considération les aspects de la rivalisation ainsi que ceux de la coopération des gouvernements dans le cyberespace, on a eu recours aux éléments de la théorie de la politique étrangère. Dans la thèse, on a présenté avant tout l'essentiel et les étapes particulières de la révolution numérique qui a abouti à la formation de l'espace téléinformatique. Ensuite, on a décrit ses traits les plus significatifs aussi bien sur le plan technique que politologique. En prenant ces éléments comme point de départ, on a tenté d'établir une typologie simplifiée de menaces téléinformatiques pour la sécurité des États qui englobe les phénomènes tels que hacking, hactivisme et cyberterrorisme. Enfin, on a analysé les exemples les plus importants de la rivalisation et coopération des États dans le cyberespace. D'une part, on a traité, entre autres, les événements qui se sont déroulés en avril et en mai 2007 en Estonie, en août 2008 en Géorgie ou ceux en Iran à partir de 2010 (Stuxnet). D'autre part, on a décrit également les différents aspects de la coopération des États dans ce domaine à l'exemple entre autres de l'Organisation des Nations Unies, de l'Union européenne, de l'OTAN et de l'Union africaine.



Dr MIRON LAKOMY – doktor nauk humanistycznych w zakresie nauk o polityce (specjalność: stosunki międzynarodowe). Absolwent politologii Uniwersytetu Śląskiego. W semestrze zimowym 2006/2007 studiował także na Université Paris Sud XI we Francji. Adiunkt w Zakładzie Stosunków Międzynarodowych Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego. Jego zainteresowania badawcze obejmują zagadnienia związane z cyberbezpieczeństwem, uwarunkowaniami konfliktów zbrojnych, a także polityką zagraniczną Francji, Polski oraz Stanów Zjednoczonych. Opublikował dotąd 2 monografie, około 40 artykułów naukowych oraz współredagował 2 prace zbiorowe. Jest stypendystą University of Cambridge (program Corbridge Trust – 2011). W 2011 roku realizował również grant badawczy International Council for Canadian Studies – *The significance of cyberspace in Canadian security policy*. Wykładał we Włoszech (Universita Degli Studi di Napoli – 2011) oraz we Francji (Université de Nice Sophia Antipolis – 2013) w ramach programu Erasmus LLP. Jest członkiem Polskiego Towarzystwa Nauk Politycznych oraz Polskiego Towarzystwa Bezpieczeństwa Narodowego.



Więcej o książce

CENA 52 ZŁ
(+ VAT)

ISSN 0208-6336
ISBN 978-83-8012-357-1